Teorie degli insiemi
Numeri ordinali e cardinali

Piero Plazzi
Dipartimento di Matematica
per le Scienze Economiche e Sociali
Università di Bologna

Indice

Introduzione: logica e teoria degli insiemi

0.1 Considerazioni storiche

L'attuale stretta connessione tra il linguaggio e i metodi della logica e quelli della matematica non è molto antica: si può dire che abbia al più un secolo, meno se si tiene conto della sua influenza sulla didattica —anche universitaria. È notevole il fatto che l'attuale situazione succede, nel lungo periodo, a posizioni molto diverse, quasi antitetiche con essa: al rifiuto della "sterilità" dei metodi logici serpeggiante tra i matematici, dal XVII secolo almeno in poi (R. CARTESIO), sia pur con grandi eccezioni (G. LEIBNIZ), alla più recente algebrizzazione della logica di G. BOOLE e di A. DE MORGAN —dunque a una influenza in senso inverso tra i due linguaggi, ormai in una forma moderna, o almeno vicina a quella d'oggi.

L'occasione per questa profonda compenetrazione di metodi fu la cosiddetta 'crisi dei fondamenti' che ha coinvolto la teoria degli insiemi di Cantor poco dopo la sua nascita e che è stata superata con una massiccia formalizzazione: questa ha portato la logica simbolica a divenire l'odierna logica matematica e ha poi fornito il linguaggio unificante —finora definitivo— per l'intera matematica: dai suoi classici domìni, abbastanza nettamente delimitati in passato, dell'algebra, della geometria, dell'analisi, alle nuove discipline annesse al corpo della matematica dopo esserne state per lungo tempo distanti ed eccentriche (valga per tutti il caso del calcolo delle probabilità), il linguaggio insiemistico provvede una uniformità di espressione mai prima sperimentata dalla matematica.

Qui si tenterà di esporre la versione corrente della teoria degli insiemi, da cui derivano, senza che spesso ne vengano esplicitati gli assiomi, i risultati fondamentali delle varie branche della matematica. Introducono alcune considerazioni di metodo e di storia, specie sui paradossi della teoria cantoriana (capitolo 1). Dopo aver esposto quella che attualmente viene considerata, con qualche variante, la teoria canonica degli insiemi (capitolo 2), vengono discussi brevemente alcuni punti cruciali dell'assiomatica, come l'assioma di scelta e l'ipotesi del continuo (capitolo 3), e viene presentata la teoria classica dei numeri ordinali e cardinali, nella versione dovuta essenzialmente a J. von Neumann (capitolo 4).

Gli assiomi, viene spesso ripetuto, costituiscono una definizione implicita della nozione intuitiva, sicché assiomatiche diverse sottointendono concezioni a volte radicalmente differenti dell'idea di insieme, così astratta e 'semplice' da poter essere precisata in molte maniere diverse, tutte però concordi nel fornire una descrizione finalizzata all'uso propriamente matematico, sia che si pensino gli insiemi come collezioni non troppo estese, dominabili come un oggetto unico (NBG) oppure come collezioni gerarchizzate per livelli di complessità (NFU), oppure come collezioni definite da condizioni 'elementari' completate da elementi ideali, una idea ricorrente nella pratica matematica (IST). Naturalmente vi sono ampie coincidenze tra queste varie teorie, confrontabili tra loro e collegate da una base condivisa per terminologia e intenti: descrizione dell'universo matematico e analisi dei suoi problemi. In questo senso si può parlare della teoria degli insiemi come di una teoria matematica e non logica, come talvolta si sostiene. Di tutto questo si è fatto cenno nell'ultimo capitolo, dedicato a una rapida rassegna di queste teorie alternative, tutte a vario titolo significative.

Si vuole dare insomma una idea non statica delle teoria degli insiemi, ma come di un campo in evoluzione, sia per quanto riguarda la ricerca propriamente assiomatica (consistenza relativa, indipendenza di assiomi), sia per le proposte (e l'approfondimento) di teorie o assiomi alternativi, sorte anche per bisogni applicativi.

0.2 Avvertenze

Agli appunti su *Computabilità, Teoremi di incompletezza, Indecidibilità* ci si riferirà con: *Appunti sulla ricorsività.* A essi si rimanda specie per nozioni di logica dei predicati. Altre convenzioni, per indici naturali ed n-uple, sono riportate nell'appendice A. L'esposizione è in genere semi-formale, come spesso per questi argomenti; soltanto in qualche caso, più che altro per fare qualche esempio di formalizzazione, si sono presentate le fbf che esprimono certi assiomi, se esse sono abbastanza semplici: in questo caso le variabili sono scritte v_i: per insiemi si sono usate lettere qualunque, tranne che nella sezione 5.2 dove, come consueto, le lettere maiuscole indicano classi e le minuscole insiemi. Secondo quanto specificato al momento opportuno, le lettere iniziali minuscole dell'alfabeto greco indicano numeri ordinali, quelle mediane numeri cardinali, seguendo l'uso.

Come in altri manuali, anche avanzati, molte dimostrazioni sono accennate, o si rimanda ad altri testi [1] . Ciò non toglie che in molti casi queste dimostrazioni si rivelino assai impegnative: il loro studio è un importante approfondimento, ma in prima battuta è forse consigliabile cogliere il senso del risultato, piuttosto che molti dettagli ingegnosi che però rischiano di essere fuorvianti per i non esperti. Questo diviene particolarmente evidente nell'ultimo capitolo, dove si è voluto dare un cenno rapidissimo a teorie alternative, più per una apertura verso i problemi odierni nel campo che per una vera e propria introduzione a questi ultimi.

[1] Alcuni manuali per gli opportuni approfondimenti sono raccolti nella bibliografia: soltanto occasionalmente, per citazioni di argomenti marginali, si sono utilizzate note a pie' pagina come questa.

In un qualsiasi testo, è quasi inevitabile che restino imperfezioni, dal semplice refuso, all'espressione non chiara e al vero e proprio errore: sarò grato a chiunque volesse segnalarmeli.

Capitolo 1

Il primo sviluppo della teoria e i paradossi

1.1 La nascita della teoria degli insiemi

Ripercorriamo a grandi linee lo sviluppo storico della teoria degli insiemi, per comprendere come si sia prodotta questa crisi dei fondamenti, partendo da una prima fase, coincidente con il periodo delle grandi scoperte cantoriane (1870-95 circa). G. Cantor fu portato allo studio di insiemi 'astratti' da problemi di analisi reale: serie di Fourier e loro domìni di convergenza, discontinuità di funzioni integrabili... La teoria astratta si sviluppò quindi a partire dallo studio di insiemi *numerici*. Nonostante l'interesse di Cantor per problemi fondazionali —allievo di Weierstraß, partecipò al processo di aritmetizzazione dell'analisi: sua è la costruzione di $\mathbb{R}$ con classi di equivalenza di successioni di Cauchy in $\mathbb{Q}$— per lui gli insiemi 'astratti' erano fondamentalmente una generalizzazione di insiemi numerici. Si spiega così la sua avversione, apparentemente contraddittoria, per gli infinitesimi, di contro alla sua rivendicazione dell'esistenza dell'infinito in atto; la tendenza a pensare gli insiemi come dotati di un ordine, nonostante l'uso, spesso, è vero, implicito, del principio di estensione; l'introduzione di nuovi concetti di numero, i *cardinali* e gli *ordinali* per mezzo di una operazione extramatematica di astrazione, e altre caratteristiche del suo pensiero, apparentemente —ma solo apparentemente— così ricco di contraddizioni. Cerchiamo di ripercorrere questa evoluzione, senza pretese di esattezza storica, ma anzi con lo scopo di vedere come i successivi assestamenti della teoria ne abbiano tratto spunto. Per una ricostruzione dell'opera e della figura di Cantor, si veda la fondamentale biografia [Dauben 1979], che seguiremo.

1.2 I primi risultati sugli insiemi numerici

L'idea che contare confrontando significasse mettere in corrispondenza biunivoca è semplicissima e molto antica: basta pensare ai conteggi 'sulle dita di una mano'; tuttavia si pensava che nel caso di conteggi e confronti tra infiniti, oltre a essere impossibile portare a termine l'operazione, si ottenessero solo antinomie legate a quel concetto intrattabile.

Così ancora Galileo, per bocca di Salviati, giudicava il fatto che i quadrati perfetti $4, 9, 16, \ldots$ si potessero mettere in tale corrispondenza con tutti i numeri $2, 3, 4, \ldots$: "*in ultima conclusione, gli attributi di eguale maggiore e minore non aver luogo ne gl'infiniti*" [1]. Un riflesso di questa prevenzione è nella definizione puramente in negativo, presente anche nell'etimologia, di 'infinito'. Il pregiudizio era legato all'atteggiamento tradizionale, registrato da Euclide stesso, di eliminazione dall'àmbito matematico del termine, almeno nella sua accezione di infinito 'attuale', come dato.

La definizione in positivo esplicitata da Dedekind, ma nota implicitamente anche in precedenza

Definizione 1.2.1. Un insieme è infinito quando lo si può mettere in corrispondenza biunivoca con un suo sottoinsieme proprio

legata anche alla sua assiomatica dei numeri naturali, non fu però sfruttata da Cantor, che semmai la usò in negativo per dare una caratterizzazione del finito [Dauben 1979, ad es. pag.178]. Partendo invece dallo studio

[1] Galileo Galilei, *Discorsi e dimostrazioni matematiche intorno a due nuove scienze*, Scienzia prima, giornata prima (1638).

del continuo numerico (oggi diremmo della struttura di $\mathbb{R}$), Cantor ottenne (1874) la straordinaria scoperta che nell'infinito si potevano fare distinzioni: si poteva in certo modo contare e fare confronti coerenti anche in questi casi.

È divenuto tradizionale esporre questo fondamentale risultato usando sviluppi decimali e applicando il *metodo diagonale* che prende il suo nome: in realtà Cantor introdusse questo metodo solo più tardi (1891) a proposito del suo teorema sulla potenza 1.2.17 [Dauben 1979, pagg.165-168]; seguiamo la dimostrazione ormai tradizionale [2].

Teorema 1.2.2. *I numeri naturali non si possono mettere in corrispondenza biunivoca con i numeri reali dell'intervallo* $[0; 1]$.

Dimostrazione. La dimostrazione è costruttiva: data una corrispondenza tra i numeri naturali (non è ovviamente restrittivo escludere lo zero) e l'intervallo $[0; 1]$ (attualmente si direbbe una funzione $f : \mathbb{N}^+ \longrightarrow [0; 1]$), si prova che essa non può essere suriettiva, tanto meno una corrispondenza biunivoca. Per far questo, si usano gli sviluppi decimali *propri* dei numeri dell'intervallo, con la sola eccezione di 1, per cui si adopera lo sviluppo improprio $1 = 0,\overline{9}$, il che assicura unicità. Continuiamo la dimostrazione in termini moderni, disponendo i valori di f in tabella:

$$\boxed{\begin{array}{lcl}
f(1) & = & 0,\mathbf{a_{1,1}}a_{1,2}a_{1,3}a_{1,4}a_{1,5}a_{1,6}a_{1,7}a_{1,8}\cdots \\
f(2) & = & 0,a_{2,1}\mathbf{a_{2,2}}a_{2,3}a_{2,4}a_{2,5}a_{2,6}a_{2,7}a_{2,8}\cdots \\
f(3) & = & 0,a_{3,1}a_{3,2}\mathbf{a_{3,3}}a_{3,4}a_{3,5}a_{3,6}a_{3,7}a_{3,8}\cdots \\
f(4) & = & 0,a_{4,1}a_{4,2}a_{4,3}\mathbf{a_{4,4}}a_{4,5}a_{4,6}a_{4,7}a_{4,8}\cdots \\
f(5) & = & 0,a_{5,1}a_{5,2}a_{5,3}a_{5,4}\mathbf{a_{5,5}}a_{5,6}a_{5,7}a_{5,8}\cdots \\
f(6) & = & 0,a_{6,1}a_{6,2}a_{6,3}a_{6,4}a_{6,5}\mathbf{a_{6,6}}a_{6,7}a_{6,8}\cdots \\
f(7) & = & 0,a_{7,1}a_{7,2}a_{7,3}a_{7,4}a_{7,5}a_{7,6}\mathbf{a_{7,7}}a_{7,8}\cdots \\
f(8) & = & 0,a_{8,1}a_{8,2}a_{8,3}a_{8,4}a_{8,5}a_{8,6}a_{8,7}\mathbf{a_{8,8}}\cdots \\
\cdots & & \ldots\ldots \\
\cdots & & \ldots\ldots
\end{array}}$$

[2] Per alcuni richiami sulle rappresentazioni e gli sviluppi decimali (o b-esimali, con b naturale maggiore di 1), come anche per gli insiemi numerici come $\mathbb{N}^+$, vedi appendice A.2.

Si può ora definire un numero x_0 dell'intervallo che ha nello sviluppo proprio una cifra differente in una posizione almeno da ogni numero della lista: se $x_0 = 0, b_1 b_2 b_3 b_4, \dots\, b_k, \dots$ si può porre

$$b_k = \begin{cases} 5 & \text{se} \quad a_{k,k} \neq 5 \\ 6 & \text{se} \quad a_{k,k} = 5 \end{cases}$$

Dunque f non è suriettiva perché x_0 non fa parte dei suoi valori. □

Il metodo prende il suo nome dall'uso che si fa della tabella, di cui si considera la 'diagonale principale': più formalmente, dall'identificazione dei due indici in $a_{h,k}$ per ottenere cifre decimali di x_0 diverse in ogni posizione.

Risultano allora tra gli insiemi numerici infiniti almeno due cardinalità (o, per usare la terminologia risalente a Cantor, *potenze*) diverse: quella del numerabile e quella del continuo. In termini moderni:

Definizioni 1.2.3.

- Si dice che un insieme A ha la potenza del numerabile se esiste una corrispondenza biunivoca tra esso e $\mathbb{N}$.
- A ha la potenza del continuo se si può mettere in corrispondenza biunivoca con $\mathbb{R}$ (e quindi, come vedremo, con un intervallo qualsiasi).
- Dal momento che esiste una corrispondenza iniettiva di $\mathbb{N}$ in $[0;1]$ ($n \mapsto \frac{1}{n+1}$), in analogia con il caso finito, si dice che un insieme numerabile ha potenza inferiore o uguale a quella del continuo; non esistendo una corrispondenza biunivoca, un insieme numerabile ha potenza *strettamente* inferiore al continuo.

Per semplici proprietà delle corrispondenze iniettive, nei confronti tra potenze di insiemi essi possono venire sostituiti da altri in corrispondenza biunivoca con essi: ad esempio, nelle definizione di sopra di potenza del numerabile, si può sostituire $\mathbb{N}$ con $\mathbb{N}^+$.

Si possono trovare abbastanza facilmente insiemi numerici significativi con la potenza del numerabile.

Proposizione 1.2.4. *I numeri interi si possono mettere in corrispondenza biunivoca con i numeri naturali.*

Dimostrazione. Basta semplicemente far corrispondere ai numeri naturali pari gli interi positivi e ai dispari i negativi:

$$g(n) = \begin{cases} \frac{n}{2} & \text{se } n \text{ è pari} \\ \frac{-n-1}{2} & \text{se } n \text{ è dispari} \end{cases} \qquad \square$$

Questo non desta grande sorpresa; ma più interessante è che

Teorema 1.2.5. *L'insieme dei numeri razionali e quello delle coppie di numeri naturali (o k-uple) si possono mettere in corrispondenza biunivoca con i naturali. Lo stesso per gli insiemi di k-uple di numeri interi o razionali.*

Dimostrazione. La prova consueta consiste in uno schema ancora una volta diagonale, dove per semplicità si rappresentano soltanto i razionali positivi, e viene suggerito un 'percorso' che permette, soppresse le frazioni non ridotte ai minimi termini (in neretto), di ottenere una corrispondenza biunivoca con i naturali:

$$\begin{array}{cccccccc}
\frac{1}{1} & \rightarrow & \frac{2}{1} & & \frac{3}{1} & \rightarrow & \frac{4}{1} & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow \\
\frac{1}{2} & & \mathbf{\frac{2}{2}} & & \frac{3}{2} & & \mathbf{\frac{4}{2}} & \dots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow \\
\frac{1}{3} & & \frac{2}{3} & & \mathbf{\frac{3}{3}} & & \frac{4}{3} & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow \\
\frac{1}{4} & & \mathbf{\frac{2}{4}} & & \frac{3}{4} & & \mathbf{\frac{4}{4}} & \dots \\
\downarrow & \nearrow & & \swarrow & & \nearrow & & \swarrow \\
\frac{1}{5} & & \frac{2}{5} & & \frac{3}{5} & & \frac{4}{5} & \dots \\
 & \swarrow & & \nearrow & & \swarrow & & \nearrow \\
\frac{1}{6} & & \mathbf{\frac{2}{6}} & & \mathbf{\frac{3}{6}} & & \mathbf{\frac{4}{6}} & \dots \\
\dots & \dots & \dots & \dots & \dots & \dots & \dots & \dots
\end{array}$$

Si possono mettere poi i razionali ≥ 0 in corrispondenza biunivoca con i numeri naturali pari e quelli negativi con i dispari: dalla dimostrazione della proposizione 1.2.4 si può poi ottenere una corrispondenza biunivoca tra i naturali e tutto $\mathbb{Q}$. Se poi non si sopprimono le frazioni non ai minimi termini, esse sono semplicemente coppie (ordinate) di numeri naturali (positivi): quindi anche $\mathbb{N} \times \mathbb{N}$ ha la potenza del numerabile; risulta poi semplice ricondursi a questo caso per le k-uple di numeri naturali (o interi, o razionali), sfruttando le precedenti corrispondenze biunivoche. $\square$

Osservando lo schema, è facile congetturare e provare un risultato largamente indipendente dai numeri in questione, ma più delicato da dimostrare del tutto in generale (vedi la discussione a proposito del teorema 3.2.20): lo enunciamo in termini moderni [Abian 1972, cap.VI, §3, Corollario 17].

Proposizione 1.2.6. *(Teorema delle unioni, caso numerabile) L'unione finita o numerabile di insiemi finiti o numerabili è anch'essa finita o numerabile.*

Intuitivamente, basta rappresentare sulle righe gli elementi di questi insiemi (non è restrittivo supporli disgiunti); vedi però il teorema citato.

Riportiamo ancora un altro notevole risultato, ottenuto anche da Dedekind con la nozione di corrispondenza biunivoca [Bottazzini 1990, cap. XII, §3, pagg.241-42].

Proposizione 1.2.7. *I numeri reali algebrici sono una infinità numerabile.*

Se passiamo agli insiemi numerici con la potenza del continuo, è immediato che

Proposizione 1.2.8. *Tutti gli intervalli si possono mettere in corrispondenza biunivoca tra loro e in particolare con la retta reale.*

Dimostrazione. Le corrispondenze biunivoche richieste sono date da funzioni elementari:

- Si possono facilmente mettere in corrispondenza biunivoca tra loro i segmenti (=intervalli limitati e chiusi) di qualunque lunghezza: si usano proiezioni (=funzioni di primo grado); lo stesso ovviamente per intervalli aperti;

- questo si estende a intervalli limitati qualunque, risultato immediato se si applica il teorema di Schröder-Bernstein citato nel séguito (teorema 1.2.11): ma si possono trovare corrispondenze elementari esplicite;
- una corrispondenza biunivoca tra un intervallo aperto ($]-\frac{\pi}{2};\frac{\pi}{2}[$) e tutto $\mathbb{R}$ è per esempio data dalla funzione tangente;
- usando ancora il teorema 1.2.11 (o funzioni elementari) si vede infine che tutti gli intervalli hanno la stessa potenza (quella del *continuo*). □

Corollario 1.2.9. *I rettangoli* $[a;b]\times[c;d]$ *hanno la stessa potenza dell'intero piano euclideo, e così per le dimensioni superiori.*

Vale poi il seguente risultato assai utile, ma non immediato:

Proposizione 1.2.10. *Se* A *è un insieme finito o ha la potenza del numerabile e* B *quella del continuo,* $C = B \setminus A$ *ha ancora la potenza del continuo.*

Dimostrazione. Vedi [Abian 1972, cap.VI, §4, Lemma 10]. □
Conseguenze notevoli sono:

Corollario 1.2.11. *Gli insiemi dei numeri irrazionali e dei numeri reali trascendenti hanno la potenza del continuo.*

Tipicamente, Cantor espresse questi due risultati non in termini astratti, ma di topologia del continuo reale. L'ultimo, poi, era tanto più notevole in quanto all'epoca si conosceva pochissimo sui numeri trascendenti, mentre esso assicurava che questi sono una infinità, e più che numerabile...

Già tutto questo era sorprendente, data la distribuzione densa dei razionali e soprattutto dei numeri algebrici sulla retta reale; ma ancora più sconcertante fu il risultato seguente.

Teorema 1.2.12. *L'intervallo unitario $I = [0;1]$ si può mettere in corrispondenza biunivoca con il quadrato unitario $\mathcal{Q} = [0;1] \times [0;1]$. Per conseguenza, la retta reale e qualsiasi spazio euclideo hanno la stessa potenza (proposizione 1.2.8 e corollario).*

Dimostrazione. La dimostrazione originale (1877, pubblicata nel 1878: [Dauben 1979, pagg.54-57]) stabilisce direttamente la possibilità di mettere in corrispondenza biunivoca spazi di dimensione qualunque. Proviamo con la stessa tecnica il caso particolare, suffciente per il risultato generale.
Si usino sviluppi decimali, con le convenzioni del teorema 1.2.2. Se un punto $P \in \mathcal{Q}$ ha coordinate

$$(0, a_1a_2a_3a_4a_5a_6a_7a_8\ldots; 0, b_1b_2a_3b_4b_5b_6b_7b_8\ldots)$$

lo si mette in corrispondenza con il numero

$$g(P) = 0, a_1b_1a_2b_2a_3b_3a_4b_4a_5b_5a_6b_6a_7b_7a_8b_8\ldots \in I.$$

Questa l'idea base della brillante dimostrazione; essa nasconde tuttavia alcuni problemi. Se infatti si prova facilmente che $g : \mathcal{Q} \to I$ è iniettiva, altrettanto immediata è la non suriettività: ad esempio, il numero $0, 0\overline{19}$ non è un valore di g.
Tuttavia, è facilissimo trovare una funzione iniettiva tra I e $\mathcal{Q}$: ad esempio, $x \in I \mapsto (x; 0) \in \mathcal{Q}$. Se l'esistenza di due distinte applicazioni iniettive in entrambi i sensi determina l'ugual potenza dei due insiemi, la dimostrazione si completa facilmente: g assicura che la potenza di $\mathcal{Q}$ è minore o uguale a quella di I, mentre per il viceversa si usa la funzione iniettiva appena citata.
$\square$
Dedekind notò questo problema, e Cantor modificò la dimostrazione, ma in modo poco soddisfacente, senza riuscire a provare l'affermazione generale [Dauben 1979, pag.172], che doveva infine venir dimostrata anni dopo da E. SCHRÖDER e, indipendentemente, da F. BERNSTEIN:

Teorema 1.2.13. *(Schröder-Bernstein) Se esistono $f : A \overset{1-1}{\to} B$ e $g : B \overset{1-1}{\to} A$, allora c'è una corrispondenza biunivoca tra A e B.*

Dimostrazione. Vedi [Abian 1972, cap.VI, §5, Teorema 35] oppure [Halmos 1980, cap.22]. $\square$
Questo teorema, già utilizzato, semplifica molte dimostrazioni: ad esempio, è un facile corollario [3]

Corollario 1.2.14. *Se A è un insieme finito o ha la potenza del numerabile e B quella del continuo, $C = A \cup B$ ha la potenza del continuo.*

Dimostrazione. Si noti che possiamo sostituire ad A, B insiemi qualsiasi con la stessa potenza, che non è restrittivo supporre disgiunti. Perciò scegliamo $A = \{1 + \frac{1}{k}; k = 1, \ldots, n\}$ (oppure $A = \{1 + \frac{1}{k}; k \in \mathbb{N}^+\}$) e $B = [0; 1]$. Si ha subito [4] $[0; 1] \hookrightarrow C \hookrightarrow [0; 2]$ e quindi C ha la potenza del continuo. $\square$
Ad ogni modo il risultato del teorema 1.2.12, mostrando che la dimensione dello spazio non influiva sulla sua potenza come insieme di punti destò grande perplessità, dato che

> sembrava distruggere la convinzione da sempre radicata nei matematici, che la dimensione di uno spazio fosse univocamente determinata dal numero di coordinate necessarie per identificare un suo punto

[Bottazzini 1990, cap. XII, §3, pag.242]. Lo stesso Cantor, comunicando il risultato a Dedekind, esclamava: "Lo vedo, ma non lo credo!". Così la dimensione e la cardinalità si avviavano ad essere distinte.

Un altro risultato in questo senso, forse meno noto, ma importante perché precorre la teoria dei frattali, è dato dall'*insieme ternario di Cantor C*: per maggiori dettagli e sviluppi, vedi [Edgar 1995]. Era ben noto che si potevano mettere in corrispondenza biunivoca segmenti di qualunque lunghezza: ma è sconcertante che abbia la stessa potenza un insieme di 'lunghezza' zero: ma questa è una delle proprietà di questo insieme.

---

[3] Vedi il teorema più generale 4.3.15.

[4] La freccia $\hookrightarrow$ indica l'inclusione insiemistica, ovviamente iniettiva.

La costruzione di C, che è un sottoinsieme di $[0;1]$, consiste in trisezioni ripetute di questo intervallo e di suoi sottointervalli, e in una applicazione, ancora una volta, della numerazione posizionale, questa volta in base 3:

Passo 1 Si triseca $[0;1] = E^{(0)}$ in tre segmenti congruenti, scartando quello intermedio (senza gli estremi); i due intervalli rimanenti $E_{1,1} = [0; \frac{1}{3}]$ e $E_{1,2} = [\frac{2}{3}; 1]$ sono costituiti dai numeri reali che in base 3 hanno una rappresentazione con prima cifra dopo la virgola diversa da 1; chiamiamo l'unione di questi due intervalli $E^{(1)}$.

Passo 2 Si ripete la trisezione in parti congruenti sui due intervalli $E_{1,1}$ e $E_{1,2}$, si scartano gli intervalli di mezzo, ottenendo 4 intervalli di lunghezza $\frac{1}{9}$, costituiti dai numeri reali che in base 3 hanno una rappresentazione con prime due cifre dopo la virgola diverse da 1 (quindi 0 oppure 2); chiamiamo l'unione di questi 2^2 intervalli $E^{(2)}$.

....

Passo $n+1$ Si ripete la trisezione in parti congruenti sui 2^n intervalli $E_{n,1} \ldots E_{n,2^n}$, di lunghezza complessiva $\frac{2^n}{3^n}$, ottenuti nel passo precedente. Si scartano gli intervalli di mezzo, ottenendo 2^{n+1} intervalli di lunghezza complessiva $\frac{2^{n+1}}{3^{n+1}}$, costituiti dai numeri reali che in base 3 hanno una rappresentazione con prime $n+1$ cifre dopo la virgola diverse da 1 (quindi 0 oppure 2); chiamiamo l'unione di questi 2^{n+1} intervalli $E^{(n+1)}$.

....

C è l'intersezione di tutti gli $E^{(n)}$ ottenuti con questi passi; è chiaro che

- C è costituito da tutti e soli i numeri di $[0;1]$ con uno sviluppo in base 3 in cui compaiono soltanto le cifre 0 e 2 (questo sviluppo è unico);
- C ha misura (lunghezza) nulla, nel senso che C si può ricoprire con intervalli di lunghezza complessiva piccola a piacere, precisamente $\frac{2^n}{3^n}$ per ogni n.

Ora si prova che C si può mettere in corrispondenza biunivoca con *tutto* l'intervallo $[0;1]$, e quindi

Proposizione 1.2.15. *Vi sono insiemi di numeri reali di misura nulla che hanno la potenza del continuo.*

Dimostrazione. L'idea della dimostrazione è ancora semplice ed elegante: dato un elemento $x_0 = 0, c_1c_2c_3c_4\dots$ di C, esso ha cifre in base 3 pari (o 0 o 2); gli si associa lo sviluppo $0, \frac{c_1}{2}\frac{c_2}{2}\frac{c_3}{2}\frac{c_4}{2}\dots$ e lo si interpreta in base 2, ottenendo un numero $y_0 \in [0;1]$. La corrispondenza $x_0 \mapsto y_0$ è *su* $[0;1]$, ma non è iniettiva; questo tuttavia dice che un sottoinsieme di C ha la potenza del continuo, e quindi per il teorema 1.2 si ha la tesi. □

Le dimostrazioni concernenti gli insiemi numerici spesso richiedono e permettono di ottenere risultati più generali, non legati ai concreti elementi degli insiemi considerati: Cantor si dedicò ora gradualmente all'approfondimento di una teoria astratta degli insiemi, motivata da sviluppi in varie direzioni, principalmente:

- la generalizzazione al caso infinito, tramite le idee di potenza e di ordine, della nozione di numero naturale, sia nell'accezione cardinale che in quella ordinale (numeri *transfiniti*);
- l'approfondimento dello studio degli insiemi numerici.

Tralasciamo per il momento la prima istanza (vedi poi il capitolo 4), anche se collegata con la seconda, e seguiamo quest'ultima. Diversi interrogativi si ponevano naturalmente:

- esistevano altre potenze di insiemi, e come andavano classificate?
- come si poteva ottenere un insieme con la potenza del continuo da un insieme con la potenza del numerabile?
- (*Problema del continuo*) esistevano insiemi di potenza intermedia tra queste?

Per risolvere questi problemi, che via via lo assorbirono sempre di più, Cantor elaborò varie strategie; soprattutto riuscì a trovare una connessione tra il continuo e il numerabile introducendo l'*insieme delle parti* (o *insieme potenza*): l'insieme di tutti i sottoinsiemi di un insieme dato.

Proposizione 1.2.16. *L'intervallo* $[0;1]$ *ha la stessa potenza dell'insieme* $\mathcal{P}(\mathbb{N}^+)$ *di tutti i sottoinsiemi di* $\mathbb{N}^+$ *(quindi di* $\mathbb{N}$*).*

Dimostrazione. Si identifichi un elemento x_0 di $[0;1]$ con il suo (unico) sviluppo binario proprio: $x_0 = 0, c_1c_2c_3c_4\ldots$ (con la solita eccezione di $1 = = 0,\overline{1}$). A x_0 si associ ora il sottoinsieme $A(x_0)$ di $\mathbb{N}^+$ definito da $A(x_0) = = \{x \in \mathbb{N}^+;\ c_x = 1\}$. L'applicazione $x_0 \mapsto A(x_0)$ è soltanto iniettiva; ma si trascura soltanto una infinità numerabile di sottoinsiemi, quelli *cofiniti* [5] , cosa che Cantor dimostra non alterare la conclusione (confronta [Dauben 1979, pagg.174-175] e il corollario 1.2.14). In alternativa a quest'ultima parte della dimostrazione, si può identificare ogni sottoinsieme $A \subseteq \mathbb{N}^+$ con la sua funzione caratteristica, intesa come successione di cifre 0 e 1, e interpretare queste come lo sviluppo *decimale* di un $x_A \in [0;1]$, ottenendo così una applicazione iniettiva $A \mapsto x_A$; si applichi poi il teorema 1.2. □

Questo risultato era il corollario di un risultato generale: data la sua importanza, ne diamo due dimostrazioni: una ricalca (adattandola e generalizzandola) la dimostrazione originale, ed è in termini di funzioni; l'altra, più corrente, risulta anche maggiormente astratta.

Teorema 1.2.17. *(di Cantor, sull'insieme potenza) Per nessun insieme* B *esiste una funzione* $g : B \xrightarrow{su} \mathcal{P}(B)$.

Dimostrazioni. (1) Vedi [Dauben 1979, pag.166]. Consideriamo una qualsiasi $g : B \longrightarrow \mathcal{P}(B)$ e identifichiamo $g(b)$, $b \in B$ con la sua funzione caratteristica $x \in B \mapsto \chi_b(x)$; si ha così una funzione di due variabili

[5] Tranne $\mathbb{N}^+$. In quanto per definizione *co*mplementari di sottoinsiemi finiti di $\mathbb{N}^+$, sono una infinità numerabile perché corrispondono ai numeri (binari) finiti. Vedi la proposizione 1.2.6, qui applicabile senza difficoltà.

$G(b;x) = \chi_b(x)$: $G(b;x) = 1 \iff x \in g(b)$. Definiamo ora una nuova funzione caratteristica per un insieme $X \subseteq B$ con $\psi(x) = 1 - G(x;x)$. Allora $X \neq g(b)$ per qualunque $b \in B$, giacché, per ogni b,

$$b \in X \iff \psi(b) = 1 \iff G(b;b) = 0 \iff b \notin g(b) \qquad \square$$

(2) Per assurdo, supponiamo che una tale funzione g esista e formiamo l'insieme $A = \{x \in B;\ x \notin g(x)\}$. Poiché $A \subseteq B$, si dovrebbe avere $A = g(c)$ per un $c \in B$. A questo punto, $c \in A \iff c \notin g(c)$: ma $g(c) = A$, da cui la contraddizione. $\square$

Si noti l'uso del metodo diagonale, che dalla prima alla seconda dimostrazione passa da una identificazione di variabili in una funzione all'identificazione di variabili in una *formula*: questa evoluzione porterà grandi risultati in logica matematica.

Da questo teorema fondamentale seguono conseguenze importanti, ad esempio l'esistenza di infiniti insiemi di cardinalità infinita sempre più grande:

Corollario 1.2.18. *Per ogni insieme B, esiste sempre un insieme di potenza maggiore: il suo insieme delle parti $\mathcal{P}(B)$.*

Dimostrazione. B si può chiaramente mettere in corrispondenza biunivoca con $\{\{z\};\ z \in B\} \subseteq \mathcal{P}(B)$; unitamente al fatto che non lo si può mettere in corrispondenza biunivoca con $\mathcal{P}(B)$ per il teorema precedente si ha la conclusione. $\square$

La definizione 1.2.3 di "potenza (cardinalità) maggiore", è stata generalizzata in maniera ovvia: vedi definizioni 4.1.1.

Dal teorema segue però anche:

Corollario 1.2.19. *Per nessun insieme B può accadere che $\mathcal{P}(B) \subseteq B$.*

Dimostrazione. Se per un insieme B risultasse $\mathcal{P}(B) \subseteq B$, una funzione $g : B \xrightarrow{su} \mathcal{P}(B)$, contro il teorema, sarebbe facilmente definibile:

$$g(z) = \begin{cases} z, & \text{se} \quad z \in \mathcal{P}(B) \\ \emptyset, & \text{se} \quad z \notin \mathcal{P}(B) \end{cases} \qquad \square$$

Questo corollario ha una conseguenza inquietante:

Nessun insieme può avere per elementi tutti gli insiemi

Dato un qualunque insieme B, almeno qualche suo sottoinsieme non gli appartiene come elemento... Ovvero,

la collezione $\mathbf{U}$ *di tutti gli insiemi non può essere un insieme*

Questa contraddizione costituisce il *paradosso di Cantor, o della classe universale*:

Paradosso di Cantor
Non esiste un insieme che abbia per elementi tutti gli insiemi

Osservazioni 1.2.20.

1. $\mathbf{U}$ viene chiamato a volte (impropriamente) insieme *universale*, o *di Cantor*; più esattamente si dovrebbe parlare di *classe* universale (vedi osservazioni 2.0.4); per ora, la indichiamo col grassetto proprio per segnalare che questa collezione *non* è un insieme.

2. Si noti che la contraddizione *non* deriva dal fatto che $\mathbf{U}$ dovrebbe contenere se stessa come elemento: dato che la relazione di appartenenza può aver luogo tra insiemi, come nel caso dell'insieme potenza, $\mathbf{U} \in \mathbf{U}$ non sarebbe di per sé contraddittorio; del resto, anche nella teoria formale è necessario un assioma apposito, non indispensabile per lo sviluppo della matematica, ad evitare fatti del genere (vedi più avanti la sezione 3.1).

Cantor per primo notò l'incongruenza, ma non le diede un peso eccessivo: congetturò che vi fossero due specie di collezioni infinite: gli insiemi, che potevano essere considerati un tutto unico, e le 'collezioni inconsistenti' che non si potevano considerare in tal modo, pena contraddizione [Dauben 1979, pagg.241-47]. Per quanto vaga, questa osservazione doveva dimostrarsi assai fruttuosa nel futuro.

1.3 La prima teoria formale e i paradossi

I risultati ottenuti da Cantor, soprattutto quelli più generali, non avevano attirato l'attenzione di molti matematici, anzi avevano suscitato in alcuni una netta ostilità, con la grande eccezione del matematico e logico G. Frege, che vi intravvide la possibilità di una fondazione puramente logica dell'intera matematica sulla base di una rigorosa teoria degli insiemi. Tralasciamo per il momento il problema della traduzione in insiemi dei numeri naturali: il processo di *aritmetizzazione dell'Analisi* del XIX secolo aveva portato a introdurre concetti potenzialmente insiemistici nella costruzione dei numeri interi, razionali, reali, complessi. Basti citare la costruzione (di Dedekind) dei numeri reali in termini di sezioni, cioè di insiemi particolari di razionali; o quella equivalente, di Cantor stesso, in termini di classi di equivalenza di successioni di Cauchy (o 'fondamentali') di razionali, ove entrano le idee di funzione, insieme, relazione e si è portati a considerare i numeri stessi come insiemi.

Nel corso di queste costruzioni, ci si accorse a poco a poco che distinguere tra insiemi e elementi non-insiemi (questi ultimi noti in letteratura come *elementi puri* o con il termine tedesco *Urelementen*) era una inutile complicazione dal punto di vista della pura fondazione della matematica; Cantor, dopo aver ottenuto i suoi fondamentali risultati sulla potenza degli insiemi numerici, era stato portato a estendere certi risultati a insiemi astratti, pur sempre pensando al problema del continuo: l'introduzione dell'insieme delle parti aveva indebolito la distinzione tra elementi e insiemi e, dopo tutto, un insieme-numero razionale può essere visto come elemento di elementi,..., di elementi di un numero reale. Così si poneva concretamente la possibilità di fondare l'intera matematica su base insiemistica. Tuttavia per far questo occorrevano definizioni rigorose —questa la critica di Frege a Cantor— di alcuni concetti fondamentali.

Cantor non dava una definizione chiara di insieme: ricorreva poi a una prima astrazione per rimuovere la natura concreta degli elementi e si richiamava a una seconda astrazione, sempre di natura psicologica, per rimuovere l'ordine (sembrava comunque pensare a insiemi numerici) e per definire la sua potenza; in tal modo, 'astraendo' si passava al 'numero cardinale' (potenza) di un insieme [Dauben 1979, pagg.156, 221]. Per rispondere a critiche di Frege, Cantor diede infine una definizione generale di insieme solo nel 1895:

> Con *insieme* intendiamo una qualsiasi riunione in un tutto unico M di ben precisi, distinti oggetti della nostra percezione o del nostro pensiero, chiamati gli elementi di M.

(tradotto da [Dauben 1979, pag.170]). Come si vede, una definizione 'psicologica' e soprattutto extramatematica, che però costituì un importante suggerimento.

Senza la pretesa di esporre l'elaborata presentazione formale, antenata degli odierni sistemi di logica matematica, proposta da Frege, vediamone alcune caratteristiche che riguardano direttamente il nostro argomento: egli, interpretando alcuni accenni di Cantor, si propose di formalizzare la teoria degli insiemi e l'intera matematica sulla base di princìpi puramente logici, espressi con grande precisione: ne consideriamo i due fondamentali. Essi equiparavano gli insiemi a *classi*, cioè alle *estensioni* di concetti (che oggi esprimeremmo con una fbf), cioè con la collezione degli oggetti (*elementi*) che possedevano una certa proprietà, espressa da quella formula; inversamente, ogni proprietà poteva determinare un insieme. Coerentemente, seguiva un principio di uguaglianza: se due insiemi possedevano esattamente gli stessi elementi, erano da considerare uguali.

1.3.1 I princìpi estensione e comprensione

Alla base di quella che si potrebbe chiamare una *prima teoria degli insiemi*, delineata implicitamente da Cantor e più formalmente da Frege e tuttora correntemente esposta nell'introdurre allo studio della teoria degli insiemi, si possono così individuare due princìpi, che non chiamiamo assiomi, per sottolinearne il carattere più logico-euristico che matematico.

Principio di estensione: Due insiemi coincidono se e solo se hanno gli stessi *elementi*
Principio di comprensione: Data una proprietà P, si possono riunire in un unico insieme A_P tutti e soli gli oggetti che godono di quella proprietà: essi sono gli *elementi* di A_P

Alcune osservazioni su questi due princìpi sono opportune, e non solo perché essi costituiscono la base, più o meno implicita, per lo sviluppo elementare della teoria, che è stata in gran parte costruita per mantenere le sue conseguenze utili in matematica ma anche 'accettabili' —nel senso di non dar luogo ai paradossi riscontrati. Si vedrà che, procedendo con la formalizzazione rigorosa di questi princìpi, si incontrano però 'paradossi' che sono vere e proprie contraddizioni: ma gli esempi e le conseguenze che esporremo ora, più o meno formalmente, rimarranno validi anche dopo l'assiomatizzazione.

Osservazioni 1.3.1. (Principio di estensione).

1. Se si ammettesse, come accennato prima, l'esistenza 'elementi puri', si dovrebbe restringere la portata del principio ai soli insiemi, altrimenti l'insieme vuoto e un non-insieme avrebbero la stessa estensione, pur essendo diversi.

2. Questo principio ha il merito di evidenziare l'unico concetto veramente fondamentale della teoria: quello di elemento —e della relativa relazione di appartenenza— cui è legato quello di uguaglianza: non a caso è mantenuto in quasi tutte le assiomatizzazioni.

3. Come sua conseguenza, e dell'uguaglianza che ne deriva, segue facilmente che

   (a) un insieme è individuato con precisione se e solo se ne vengono determinati gli elementi: in questo senso, è un principio di *unicità*.

   (b) Se l'insieme A ha per elementi $a, b, \ldots, z$ (in numero finito e ... piccolo!) ma nessun altro, esso è quindi ben definito per enumerazione: lo si indica con $\{a; b; \ldots ; z\}$: si parla di rappresentazione *tabulare* di A.

(c) Ancora, il principio comporta che differenti descrizioni degli elementi di un insieme, loro eventuali ripetizioni o enumerazione di essi in altro ordine *non* cambi l'insieme: se A ha per elementi esattamente i numeri naturali $0, 1, 2$ si ha indifferentemente

$$A = \{0; 1; 2\} = \{0; 1; 1{+}1\} = \{0; 2; 1\} = \{1; 2; 0\} = \{2; 1; 1; 0; 0; 2\}$$

Come si è visto, Cantor presupponeva invece, più o meno esplicitamente, un certo ordine tra gli elementi.

4. Tuttavia, il principio permette di riconoscere soltanto l'uguaglianza di insiemi già dati, non ne garantisce in nessun modo l'*esistenza*: naturalmente i semplicissimi insiemi elencati sopra non danno alcun problema, ma proprio l'esistenza (come insiemi) di collezioni di oggetti può dare problemi di consistenza per la teoria.

Osservazioni 1.3.2. (Principio di comprensione).

1. Questo secondo principio garantisce appunto l'esistenza come insiemi di certe collezioni di oggetti; correlata a questo è la rappresentazione *caratteristica* di un insieme: con i simboli usati più sopra, si rappresenterebbe A_P con $\{x; x \text{ ha la proprietà } P\}$ o, più sinteticamente, con $\{x; P(x)\}$. Si può procedere con la formalizzazione se si esprime la proprietà P con una fbf $\phi(u)$ [6] di un opportuno linguaggio predicativo —è anche possibile introdurre con altre variabili libere $u_1, \ldots, u_n$ degli ulteriori 'parametri' nella definizione: si scrive allora

$$A_P = \{u; \phi(u; u_1, \ldots, u_n)\}$$

Intuitivamente, A_P è un insieme che dipende dai 'parametri' ${}^n u$.

[6] Per i simboli e le convenzioni logici, nonché per quelli sugli indici, vedi *Appunti sulla ricorsività*, Appendice A e capitolo 2.

2. L'uso di variabili permette di descrivere insiemi infiniti; la rappresentazione caratteristica è infatti l'unica adatta a rappresentare questi insiemi; ma è anche assai comoda per insiemi finiti con molti elementi.

$$A = \{x;\ x \text{ è un numero naturale primo minore di } 10^{30}\}$$

Esempi 1.3.3. 1. Esiste in base al principio di estensione un *unico* insieme vuoto, cioè senza elementi; la sua esistenza è garantita dal principio di comprensione, mediante la proprietà 'essere diverso da se stesso': $x \neq x$. Pertanto gli si può attribuire correttamente un simbolo di costante: $\emptyset$.

2. Proprietà diversissime, che sarebbe irragionevole identificare, danno luogo a insiemi uguali per estensione:

$$\{7; 11\} = \{x; x \text{ è un primo compreso tra 6 e 12}\} = \{x; x^2 - 18x + 77 = 0\}$$

3. Addirittura, due insiemi possono essere uguali o no per estensione, senza che lo si possa decidere, almeno allo stato attuale delle conoscenze. Facciamo un esempio ben noto, la congettura di Goldbach:

Ogni numero pari ≥ 4 *è somma di due numeri primi*

Al momento non si ha una dimostrazione né una refutazione di questo enunciato, e quindi non è noto se

$$\emptyset = \{x; x \geq 4 \text{ è pari, ma non è somma di due numeri primi}\}$$

nonostante che i due insiemi siano ben definiti per comprensione.

1.3.2 Il paradosso di Russell

Frege intendeva dare un contenuto preciso alle intuizioni di Cantor e un fondamento logico all'intera matematica mediante una versione formale dell'astrazione: ad esempio, il numero 'tre' sarebbe sorto non per astrazione psicologistica, ma come classe di tutti gli insiemi in corrispondenza biunivoca con $\{a; b; c\}$, classe detreminata da una precisa proprietà mediante il principio di comprensione. In effetti tutta la teoria degli insiemi e l'intera matematica si potrebbero dedurre dai due princìpi di estensione e comprensione con dimostrazioni formalmente corrette: purtroppo, ciò è dovuto al fatto che *questi princìpi sono contraddittori.*

Già l'idea di insieme delle parti aveva prodotto, con il proliferare di insiemi infiniti di potenza sempre maggiore, un paradosso. Dal fondamentale teorema 1.2.17 segue, come si è visto, l'esistenza di infiniti insiemi di cardinalità infinita sempre più grande, ma anche una conseguenza inquietante: nessun insieme può avere per elementi tutti gli insiemi. Cantor aveva risolto a suo modo il paradosso accennando alla esistenza di 'molteplicità inconsistenti' accanto ai veri e propri insiemi, 'molteplicità consistenti', ma senza chiarire la distinzione, che rimaneva un dato di fatto senza spiegazione. Il principio di comprensione però sembra assicurare l'esistenza di un tale insieme, dato che la proprietà "essere un insieme" è perfettamente legittima: la si può formalizzare con $x = x$. Questa vera e propria contraddizione costituisce il paradosso di Cantor (vedi pagina 21, con le relative osservazioni). Si potrebbe pensare che la contraddizione derivi dall'ammissione che i sottoinsiemi di qualsiasi insieme costituiscano un insieme, e quindi dalla equiparazione di elementi e insiemi; ma il problema è più profondo, come mostra il

Paradosso di Russell
Non esiste un insieme che contenga tutti gli insiemi che non *contengono se stessi come elemento*

□ Infatti, se $\mathbf{R} = \{x;\ x \notin x\}$, ci si chiede se $\mathbf{R} \in \mathbf{R}$ o no: per estensione, questo dovrebbe avere una risposta ben precisa, ma entrambe portano a una contraddizione visto che, per definizione $\mathbf{R} \in \mathbf{R} \Longleftrightarrow \mathbf{R} \notin \mathbf{R}$. □

Ma per il principio di comprensione, $\mathbf{R}$ dovrebbe pur essere un insieme: di qui una vera e propria contraddizione. Questo paradosso è di natura puramente logica: infatti ha validità logica la fbf

$$\neg\exists v_0 \forall v_1 (R(v_1\,; v_0) \Leftrightarrow \neg R(v_1; v_1))$$

dal momento che essa risulta vera comunque si interpreti, non necessariamente come appartenenza insiemistica, il predicato binario R. In effetti, proprio per la sua generalità, esso è molto potente: ne segue tra l'altro anche il paradosso di Cantor (vedi sotto, teorema 2.1.7).

Questo paradosso dunque colpiva soprattutto il tentativo di Frege, quasi portato a termine dopo molti anni, di ridurre a concetti logici generali la matematica usando la teoria degli insiemi, visti come classi secondo la tradizione logica.

> A uno scrittore di scienza ben poco può giungere più sgradito del fatto che, dopo completato un lavoro, venga scosso uno dei fondamenti della sua costruzione. Sono stato messo in questa situazione da una lettera del signor Bertrand Russell [...] [7]

Con queste parole Frege annunciava la comunicazione del paradosso, riconoscendone, con esemplare correttezza scientifica, l'importanza in negativo per la sua opera: si apriva così la 'crisi dei fondamenti', un periodo di incertezza sia sui metodi logici tradizionali che sulla correttezza delle dimostrazioni matematiche. Mentre Russell si dedicava a continuare l'opera di Frege, molti matematici, soprattutto Hilbert e la sua scuola, si dedicarono a riformulare i procedimenti logici specifici della dimostrazione matematica e in particolare ad affinare i princìpi della teoria degli insiemi, per giustificare e approfondire le scoperte di Cantor. Gli insiemi si rivelarono classi molto particolari, dotate di proprietà specifiche: la formulazione assiomatica fu messa a punto sulla base dell'opera di E. ZERMELO, completata da A. FRAENKEL, da cui il nome del sistema standard per la teoria contemporanea degli insiemi: ZF, che considereremo nel prossimo capitolo.

[7] Traduzione italiana di C. Mangione, [Mangione 1975, §4.4].

Capitolo 2

La teoria assiomatica ZF

La presenza (e il proliferare) di paradossi nell'àmbito della prima formulazione della teoria di Cantor, nonostante la veste rigorosa che aveva tentato di darle Frege, richiesero la precisazione dei metodi dimostrativi e degli assiomi usati, mutando indirettamente anche il concetto di insieme, semplice solo in apparenza. La revisione fu condotta seguendo l'intuizione di Cantor che i paradossi fossero dovuti alla possibilità di formare come insiemi collezioni troppo numerose, impossibili da concepire come "un tutto unico" senza incorrere in contraddizione. Di conseguenza venne abbandonato il principio di comprensione nella sua forma non ristretta, permettendone l'applicazione soltanto in casi ben precisi.

Per la formalizzazione venne sviluppato l'odierno linguaggio della logica dei predicati, dovuto a D. Hilbert e alla sua scuola: la teoria più diffusa è infatti quella sviluppata da E. Zermelo (e A. Fraenkel), da cui la sigla ZF con cui il sistema in questione viene comunemente citato. Zermelo fu portato inizialmente a formulare una versione assiomatica della teoria per giustificare un teorema da lui dimostrato (teorema 3.2.2), teorema chiave per la teoria dei numeri cardinali e ordinali, mettendone in chiaro tutte le premesse; ma la forma e l'esigenza stessa dell'assiomatizzazione provenivano dalla situazione creatasi coi paradossi, che richiedevano un grado di rigore superiore a tutti i precedenti.

In maniera semiformale, ma formalizzabile, esponiamo gli assiomi che costituiscono (a volte con qualche variante) questa teoria e, almeno nei casi più semplici, la loro versione completamente formale (ZF propriamente detta).

Osservazioni 2.0.4.
- Si è accennato al fatto che possiamo considerare in tutta la teoria soltanto insiemi: si riesce comunque a inquadrare tutta (o quasi) la matematica attuale e, del resto, questo è coerente con la costruzione degli insiemi numerici a partire dai numeri naturali: per questi, vedi la definizione 2.2.11.

- Informalmente, useremo dunque senza sistematicità variabili —lettere maiuscole o minuscole— $a, b, c \ldots, x, y, z, A, B, C, \ldots$, solo per insiemi: si potrebbero distinguere i non-insiemi mediante altri tipi di variabile, o introdurre un predicato M apposito ($M(x)$ per 'x è un insieme'): ma queste complicazioni non apporterebbero approfondimenti particolari.

- Il tipico simbolo delle parentesi graffe (*classificatore*) determina una classe a partire da una formula, che è da chiamare insieme (un termine della teoria) se gli assiomi lo consentono; la x di $\{x; \ldots\}$ si comporta come una variabile vincolata.

- Alle classi 'troppo numerose', che possono creare contraddizione, è ora permesso comparire nella teoria solo come predicati, anche se questi possono venire rappresentati come enti estensionali per aiutare l'intuizione. Facciamo l'esempio della classe universale di Cantor, legata al predicato $v_0 \equiv v_0$: essa viene rappresentata come $\{x; x = x\}$, ma non deve essere pensata come un insieme! Per non confonderla con questi (è una *classe propria*), la si indica con il grassetto: si scrive $\mathbf{U}$ e $x \in \mathbf{U}$ equivale a $x = x$. Lo stesso per tutte le estensioni che potrebbero non essere giustificabili come insiemi.

- La semantica della teoria formale può lasciare perplessi: interpretiamo la teoria degli insiemi con strutture basate su insiemi! Bisogna a questo punto chiarire che le interpretazioni saranno fatte dando per scontata la possibilità di usare senza contraddizioni insiemi finiti o al massimo $\mathbb{N}$ o simili. Non c'è circolo vizioso se ci limitiamo a giustificare l'esistenza (sempre nel senso di non contraddittorietà) di insiemi problematici mediante insiemi molto semplici, della cui esistenza non si dubita affatto.

- La teoria permette di *provare* che certe collezioni o classi sono insiemi: perciò la frase 'esiste per (o: in) ZF il tale insieme' significa soltanto 'la tal collezione è (si può considerare) un insieme' —nel senso della definizione implicita data dagli assiomi.

ZF è a rigor di termini una teoria del primo ordine con uguaglianza $\equiv$ e unico simbolo proprio $\in$ per predicato binario, usato infisso. Tutti gli altri simboli usati vengono introdotti in un secondo tempo con definizioni. Nel séguito la presentazione sarà spesso soltanto semi-formale. Ancora, è utile usare *quantificazioni limitate* su insiemi a o su classi $\mathbf{M}$ (fbf):

- $\forall x \in a\ \phi$ abbrevia $\forall x(x \in a \Rightarrow \phi)$
  $\forall x \in \mathbf{M}\ \phi$ abbrevia $\forall x(\mathbf{M}(x) \Rightarrow \phi)$

- $\exists x \in a\ \phi$ abbrevia $\exists x(x \in a \wedge \phi)$
  $\exists x \in \mathbf{M}\ \phi$ abbrevia $\exists x(\mathbf{M}(x) \wedge \phi)$

Si noti che in questo modo si introducono nuove variabili libere (ad esempio, a), a meno che non si usino costanti per indicare ben precisi insiemi.

2.1 Gli assiomi di estensione e specificazione

Il primo assioma, di estensione, è esattamente il principio già esposto, formalizzato nel linguaggio:

Assioma di estensione [E] Due insiemi coincidono se e solo se hanno gli stessi elementi
$\forall v_0 \forall v_1 (v_0 \equiv v_1 \iff \forall v_2 (v_2 \in v_0 \iff v_2 \in v_1))$

Valgono naturalmente le osservazioni 1.3.1 già fatte al proposito. Inoltre:

Osservazioni 2.1.1.

1. La parte dell'assioma con una implicazione verso destra, $\forall v_0 \forall v_1 (v_0 \equiv v_1 \implies \forall v_2 (v_2 \in v_0 \iff v_2 \in v_1))$ è semplicemente una espressione della sostitutività di $\equiv$; l'altra implicazione costituisce il vero e proprio assioma.

2. Data la sua forma, si può addirittura usare questa fbf come *definizione* di $\equiv$: occorrerebbe però un'altra formulazione di E: vedi, sia pure in un contesto più generale, [Mendelson 1972, pagg. 196-97].

Schema di specificazione, o dei sottoinsiemi [S] Dati un insieme a e una proprietà (fbf) ϕ, la collezione degli $x \in a$ che soddisfano ϕ è un insieme
$\forall v_0 \exists v_1 \forall v_2 (v_2 \in v_1 \iff (v_2 \in v_0 \wedge \phi))$

Se a è un insieme e $\phi = \phi(x)$ una proprietà, esiste (per S) ed è unico (per E) l'insieme b degli $x \in a$ per cui $\phi(x)$ vale; ciò giustifica il consueto simbolo $\{x \in a;\ \phi(x)\}$ con le parentesi graffe (il *classificatore*) per indicare b. Si noti che, a rigore, non si può omettere l'insieme ambiente a, perché si ricadrebbe nel pieno principio di comprensione.

Si riconosce immediatamente che b è un sottoinsieme di a, nel senso della

Definizione 2.1.2. Quando ogni elemento di a è anche elemento di c, cioè $\forall z (z \in a \implies z \in c)$, si dice che $a \subseteq c$. Se poi $a \neq c$ —in altre parole, se esiste uno $z \in c$ tale che $z \notin a$, a è un sottoinsieme *proprio* di c: $a \subset c$. I relativi simboli sono i simboli di *inclusione*.

Con E, S risulta assai facile provare semplici proprietà dell'inclusione, come ad esempio

- per ogni a: $\emptyset \subseteq a$ e $a \subseteq a$;
- per ogni a, b, c: $(a \subseteq b \wedge b \subseteq a) \Leftrightarrow a = b$ e $(a \subseteq b \wedge b \subseteq c) \Rightarrow a \subseteq c$,

eccetera.

Inoltre, dal momento che dagli assiomi dell'uguaglianza segue $\exists v_0(v_0 \equiv v_0)$, sia c un insieme; si considera $\{x \in c;\ x \not\equiv x\}$ (vedi l'osservazione sopra); si prova che questo insieme non cambia cambiando c (per E) e quindi si può definire l'*insieme vuoto* $\emptyset$:

Definizione 2.1.3. $\emptyset = \{x \in c;\ x \not\equiv x\} = \{x;\ x \not\equiv x\}$

Come si vede, in certi casi si può ancora applicare il principio di comprensione puro e semplice.

Osservazioni 2.1.4.

1. Questa forma S limitata del principio è uno schema di infiniti assiomi, dato che se ne ottiene uno per ogni *fbf* ϕ: in essa possono occorrere libere v_0, v_2 e altre variabili, nel qual caso per avere enunciati si considera assioma la relativa chiusura universale, *ma non* v_1. Infatti, se ciò fosse possibile, si avrebbe un assioma
$$\forall v_0 \exists v_1 \forall v_2 (v_2 \in v_1 \Longleftrightarrow (v_2 \in v_0 \wedge \neg v_2 \in v_1))$$
che impone che ogni insieme sia (l'insieme) vuoto!

2. Lo schema S si chiama 'dei sottoinsiemi' dal momento che è permesso applicare il principio di comprensione soltanto all'interno di un insieme ambiente a già formato. Può sembrare una limitazione leggera, ma in effetti con gli assiomi E ed S è possibile definire l'insieme vuoto ma *questo soltanto.* Infatti se si interpreta il linguaggio insiemistico in un ambiente con un solo oggetto ζ dove la relazione $\in$ è la relazione vuota, si vede che E ed S sono soddisfatti, e quindi questo è un modello (normale) di essi. Dunque, da E ed S non si può derivare l'esistenza di

insiemi non vuoti: $E, S \nvdash \exists v_0 \exists v_1 (v_1 \in v_0)$. In compenso E ed S hanno un modello e quindi *sono un sistema consistente.*

Si possono comunque dare in base a questi assiomi già alcune altre definizioni.

Definizioni 2.1.5.

- (Intersezione) $a \cap b = \{x \in a; x \in b\}$ è l'intersezione (booleana) di a con b;
- (Differenza e complementare) $a \setminus b = \{x \in a; x \notin b\}$ è la differenza insiemistica di a con b.
  Se $b \subseteq a$, $a \setminus b = \complement_a b$ è il complementare di b in a.

Per quanto riguarda l'intersezione, la si può eseguire tra insiemi di una famiglia [1] $\mathcal{F}$ non vuota di insiemi, e addirittura su una collezione $\mathbf{M}$ di insiemi caratterizzati da una certa proprietà, anche se questa non costituisce un insieme ma soltanto una classe propria, sempre purché questa non sia vuota: se $c \in \mathbf{M}$ (cioè vale $\mathbf{M}(c)$), oppure $c \in \mathcal{F}$, si pone

Definizione 2.1.6.

$$\bigcap \mathcal{F} = \bigcap_{x \in \mathcal{F}} x = \{z \in c; \forall x \in \mathcal{F}\ z \in x\}$$

$$\bigcap \mathbf{M} = \bigcap_{x \in \mathbf{M}} x = \{z \in c; \forall x \in \mathbf{M}\ z \in x\}$$

La richiesta $\mathbf{M} \neq \emptyset$ (o $\mathcal{F} \neq \emptyset$) è indispensabile: senza c non si potrebbe applicare S e si otterrebbe infatti la classe universale $\mathbf{U}$. Naturalmente l'insieme ottenuto è indipendente dal c scelto.

Si è già visto il paradosso di Russell (sottosezione 1.3.2); è interessante notare a questo punto che, solo da E ed S, dalla stessa *fbf* $x \notin x$ segue il paradosso di Cantor, *senza usare la costruzione dell'insieme potenza*:

[1] Si usa questa parola come sinonimo di insieme, soltanto per evitare la ripetitiva espressione 'insieme di insiemi' e sostituirla con 'famiglia di insiemi'.

Teorema 2.1.7. *Se a è un insieme qualsiasi, $r(a) = \{x \in a;\ x \notin x\}$ non può essere elemento di a: quindi nessun insieme contiene tutto e* **U** *non può essere un insieme.*

Dimostrazione. Se fosse $r(a) \in a$, si avrebbe $r(a) \in r(a) \Leftrightarrow r(a) \notin r(a)$, contraddizione. □

L'*insieme di Russell per a*, $r(a)$, è ben definito in ZF per S.

Esercizio 2.1.8. Come si interpreta questo paradosso nel modello precedente ove esiste solo un 'insieme' vuoto?

2.2 Gli assiomi della coppia, dell'unione, della potenza

Come si è visto, il sistema costituito da E ed S (si scrive a volte $\{E; S\}$) non permette nemmeno di provare l'esistenza di un singolo insieme non vuoto. Bisogna perciò aggiungere altri assiomi di esistenza, che permettano le consuete costruzioni insiemistiche. Seguono allora a questo punto tre assiomi, accomunati da questa caratteristica e anche dalla analogia dei loro enunciati, anche se molto diversi per portata.

Assioma della coppia [C]
Dati a e b qualunque, esiste sempre un terzo insieme c che li contiene come elementi: $a \in c$ e $b \in c$
$\forall v_0 \forall v_1 \exists v_2 (v_0 \in v_2 \wedge v_1 \in v_2)$

Assioma dell'unione [U]
Dato un insieme a qualunque, esiste sempre un insieme c che contiene come elementi tutti gli elementi di elementi di a: $d \in b$, $b \in a$ implicano $d \in c$
$\forall v_0 \exists v_1 \forall v_2 \forall v_3 ((v_2 \in v_3 \wedge v_3 \in v_0) \Rightarrow v_2 \in v_1)$

Assioma della potenza [P]
Dato un insieme a qualunque, esiste sempre un insieme c che contiene come elementi tutti i sottoinsiemi di a: $b \subseteq a$ implica $b \in c$
$\forall v_0 \exists v_1 \forall v_2 (v_2 \subseteq v_0 \Rightarrow v_2 \in v_1)$

Con E ed S questi assiomi permettono di definire *coppie non ordinate*, *unioni* e *insiemi potenza*:

Definizioni 2.2.1. 1. Dati insiemi a e b, se c è come in C,

$$\{z \in c;\ z = a \vee z = b\} = \{z;\ z = a \vee z = b\}$$

è la coppia *non ordinata* di elementi a e b; se $a = b$, $\{a; b\}$ coincide per estensione con $\{a\}$: è il *singoletto* (o *singleton*) di a.

2. Dato un insieme (famiglia) a di insiemi, se c è come in U,

$$\{z \in c;\ \exists b(z \in b \wedge b \in a)\} = \{z;\ \exists b(z \in b \wedge b \in a)\} = \bigcup a$$

è l'unione degli elementi di a.

3. Dato un insieme a, se c è come in P,

$$\{z \in c;\ z \subseteq a\} = \{z;\ z \subseteq a\} = \mathcal{P}(a)$$

è l'insieme potenza (o: delle parti) di a.

Le definizioni sono corrette in ZF, dato che gli insiemi introdotti non variano con c, per estensione. Si è messo in evidenza il fatto che queste definizioni sono casi particolari di comprensione, applicata a speciali fbf.

2.2.1 Coppie, relazioni, funzioni

Se $\{a; b\}$ è una coppia non ordinata, per l'assioma di estensione si ha $\{a; b\} = \{b; a\}$, da cui il nome, ma con un semplice artificio si può ottenere che la coppia 'registri' l'ordine dei due elementi:

Definizione 2.2.2. La coppia ordinata di componenti (o coordinate) a e b (rispettivamente prima e seconda) è $(a;b) = \{\{a\};\{a;b\}\}$.

Questa definizione, dovuta a K. Kuratowski, è sì artificiosa, e potrebbe essere formulata in altri modi ottenendo lo stesso risultato qui sotto, ma risulta molto utile, perché permette di aggirare l'assioma di estensione e rappresentare l'ordine nella teoria. Infatti vale il

Teorema 2.2.3. $(a;b) = (c;d)$ *se e solo se le componenti sono ordinatamente uguali:* $a = c$ *e* $b = d$.

Possiamo anche introdurre le n-uple come particolari coppie ordinate (d'ora in poi, 'coppie' semplicemente):

Definizione 2.2.4. Una tripletta (ordinata) $(a;b;c)$ è per definizione una particolare coppia $((a;b);c)$. In generale si procede per induzione: se $n \geq 3$, una n-upla (ordinata) $(a_1;\ldots;a_n)$ è una particolare coppia $((a_1;\ldots;a_{n-1});a_n)$.

Per uniformità, si può definire una 1-upla (a) semplicemente come a: del resto, si usano anche altre definizioni di n-upla, equivalenti a meno di una *corrispondenza canonica*; i vari insiemi ottenuti vengono *identificati* con quelli dati sopra: vedi osservazioni 2.2.15.

Soprattutto, si può definire cosa si intende per relazione e per funzione:

Definizione 2.2.5.

1. Una relazione (binaria) R è un insieme di coppie ordinate; una relazione n-aria è un insieme di n-uple; nel caso $n = 1$ si ha un semplice insieme e non si adopera il termine.

2. Si può ora indicare come al solito cosa significhino le varie proprietà delle relazioni e quindi definire relazioni di equivalenza, di ordine e funzioni.

3. Una funzione è una relazione f *univoca*: se $(a;b_1)$, $(a;b_2) \in f$ si ha $b_1 = b_2$. Questo permette di definire il valore y di f in x: se $(x;y) \in f$ questo valore si indica con $f(x)$: $y = f(x)$. Formalmente $f(x)$ è un

simbolo funzionale di *due* variabili, che richiede una adeguata definizione per ogni coppia di insiemi f, x: ad esempio $y = f(x)$ se e solo se si ha $\exists! y\ (x; y) \in f$ e $y = \emptyset$ (un valore di comodo) altrimenti.

4. Una funzione g è iniettiva (o: 1-1) se $(a_1; b)$, $(a_2; b) \in g$ implicano $a_1 = a_2$. $\square$

Vedi altra terminologia qui sotto (osservazioni 2.2.2) e in Appendice, A.3.1 e A.3.2.

Osservazioni 2.2.6.

- Le relazioni n-arie ($n > 2$) sono particolari relazioni binarie, sicché nella teoria si può parlare soltanto di queste ultime, sottointendendo 'binarie';
- per queste relazioni spesso si usa la notazione infissa: aRb anziché $(a; b) \in R$. Viene usata anche la notazione $R(a; b)$: vedi *Appunti sulla ricorsività.*
- La definizione insiemistica di funzione la identifica con il suo grafico, che usualmente viene distinto da essa, come ad esempio in analisi o in teoria della ricorsività (ancora, vedi *Appunti sulla ricorsività*).

2.2.2 Unioni, domini, immagini, restrizioni

La definizione, la terminologia e il simbolo di unione sono differenti da quelli usati correntemente: ma vi si riportano facilmente. Anzitutto, si parla di solito di unione di una *famiglia* di insiemi: il termine, come si è già detto, è un semplice sinonimo di 'insieme'. Si ricordi che in ZF si parla soltanto di insiemi. Vediamo alcuni casi particolari di unioni e loro propietà:

- $\cup\{a; b\}$ è costituita per definizione dagli elementi di a o di b: quindi $\cup\{a; b\} = a \cup b = \{x;\ x \in a \vee x \in b\}$: si riottiene la solita definizione (di unione *booleana*). Iterando poi l'unione di due insiemi, si ottiene che:

- se sono dati insiemi in numero finito qualunque $n > 1$, siano $a_0, \dots, a_n$, esiste $a_0 \cup \dots \cup a_n = \cup_{j=0}^{n} a_j$;
- se gli a_j precedenti sono singoletti $\{x_j\}$, esiste sempre l'insieme finito $\{x_0; \dots; x_n\}$, comunque si scelgano i suoi $n+1$ elementi x_j.

- Un caso banale è $\cup\{a; a\} = \cup\{a\} = a \cup a = a$ (idempotenza dell'unione). Quindi $\cup\{\emptyset\} = \cup\emptyset = \emptyset$.

Può stupire il fatto che, mentre di solito unione e intersezione sono trattate simmetricamente, qui vi sia un apposito assioma per le unioni: ciò è dovuto alla impostazione di fondo dell'assiomatica, tesa a evitare la formazioni di collezioni 'troppo numerose': mentre con intersezioni anche su intere classi questo non può accadere, sarebbe questo il caso di unioni troppo estese. Si noti tuttavia che si può ammettere *come classe* una unione su una classe propria $\mathbf{C}$ di insiemi: la si può infatti rappresentare come estensione della *fbf* $\exists y(\mathbf{C}(y) \wedge x \in y)$: $\cup\mathbf{C} = \{x;\ \exists y(\mathbf{C}(y) \wedge x \in y)\}$. Vedi la sezione 5.2.

Consideriamo ora una relazione R e sia $(a; b) \in R$. Allora

$$a, b \in \{a; b\} \in (a; b) \in R, \quad a, b \in \{a; b\} \in \bigcup R, \quad a, b \in \bigcup\bigcup R;$$

possiamo dunque definire come insiemi dominio e immagini di una relazione:

Definizioni 2.2.7. • Il dominio di R è

$$dom(R) = \{a \in \bigcup\bigcup R;\ \exists b \in \bigcup\bigcup R, (a; b) \in R\}$$

- L'immagine di R è

$$Im(R) = \{b \in \bigcup\bigcup R;\ \exists a \in \bigcup\bigcup R, (a; b) \in R\}$$

- La restrizione di R a un sottoinsieme a_0 del suo dominio è la relazione

$$R \restriction a_0 = \{z \in R;\ \exists u \exists v(z = (u; v) \wedge u \in a_0)\}.$$

- L'immagine $R[a_0]$ di a_0 tramite R è l'immagine della sua restrizione:

$$R[a_0] = Im(R \restriction a_0).$$

Osservazioni 2.2.8.
- Queste definizioni hanno senso anche per insiemi R (e a_0) qualunque, ma sono particolarmente significative per *funzioni*, che nel séguito indicheremo come al solito con f, g.

- Si noti che conviene distinguere tra i *valori* $f(x)$, $x \in dom(f)$, e le *immagini* $f[a_0]$, $a_0 \subseteq dom(f)$, differenziando le parentesi: è infatti possibile che un elemento del dominio ne sia anche sottoinsieme, generando ambiguità: ad esempio, se $\emptyset \in dom(f)$, sarà anche $\emptyset \subseteq dom(f)$.

- Se $dom(f) = a$ e $Im(f) \subseteq b$ si scrive anche $f : a \to b$ (b è un *codominio* di f). Se $b = Im(f)$, si dice che f è *su* b, o che è *suriettiva* (in simboli: $f : a \stackrel{su}{\to} b$); mentre però la eventuale iniettività risulta una caratteristica intrinseca alla funzione, la suriettività dipende dal codominio che non è, a differenza dell'immagine, determinato univocamente da f.

- Se f ha dominio a, immagine b (e quindi è su b), si dice che è una biiezione (o una corrispondenza biunivoca) tra a e b.

Usando funzioni è possibile definire le unioni su *famiglie indicizzate* di insiemi, come nella usuale notazione.

Definizione 2.2.9. Una funzione $f : a \stackrel{su}{\to} b$ in questo contesto si dice una *indicizzazione* della famiglia b e gli elementi $x \in a$ si dicono i relativi *indici*: poi si scrive

$$\bigcup b \quad \text{come} \quad \bigcup_{x \in a} f(x)$$

Se anziché $f(x)$ si scrive b_x si ha il simbolo ancor più familiare $\bigcup_{x\in a} b_x$; eccetera.

Vediamo ora come si possano rappresentare i numeri naturali come particolari insiemi; questo dipende da una costruzione del tutto generale, quella di *successore* di un insieme:

Definizione 2.2.10. Il successore (insiemistico) di un insieme a è l'insieme $S(a) = a \cup \{a\}$, indicato anche semplicemente con Sa.

Si possono ora definire per induzione nel metalinguaggio i *numerali di von Neumann* [2], corrispondenti insiemistici dei numeri naturali.

Definizione 2.2.11. Il numerale zero, $\overline{0}$, è $\emptyset$; supposto di aver definito il numerale $\overline{m}$, il numerale $\overline{m+1}$ è $S(\overline{m}) = \overline{m} \cup \{\overline{m}\}$.

Si ha ad esempio $\overline{1} = S\overline{0} = \{\overline{0}\}$, $\overline{2} = S\overline{1} = \{\overline{0}; \overline{1}\}$, eccetera. Chiarito che si tratta di *insiemi*, si scrivono di solito senza sopralineatura: $1 = \{0\}$, $2 = \{0; 1\}$ e, in generale, $m + 1 = \{0; 1; \ldots; m\}$. L'insieme m ha dunque sempre m elementi: i suoi predecessori. Nessuno degli assiomi fin qui incontrati assicura però di poter riunire in un unico insieme tutti questi insiemi: di fatto è necessario un assioma apposito —vedi oltre, sezione 2.4.

Osservazioni 2.2.12.

- Finora sono stati introdotti molti nuovi simboli tra cui simboli predicativi, come ad esempio quello per sottoinsieme: è bene allora osservare che i simboli predicativi (incluso $\in$) non determinano affatto relazioni in senso insiemistico; l'inclusione $\subseteq$ o l'appartenenza $\in$ avrebbero per dominio $\mathbf{U}$, cosa impossibile per una relazione intesa come insieme. Certamente in un modello degli assiomi un predicato, ad esempio quello di inclusione, determina una relazione e lo stesso avviene quando lo restringiamo a una famiglia di insiemi; ma a rigore non è corretto, e soprattutto è fuorviante, parlare di '*relazione* di inclusione'. Per evitare queste ambiguità sarebbe preferibile parlare di 'predicato di inclusione' o, allo stesso modo, di 'proprietà' nel caso di un argomento.

- Sono stati introdotti anche molti nuovi simboli per costante (come $\emptyset$ o i numerali) e nuovi simboli funzionali: tali sono i simboli di intersezione (per due insiemi), di successore, eccetera. Il caso dei simboli funzionali

[2] Vedi *Appunti sulla ricorsività.*

è analogo al precedente ma ancor più fuorviante. Consideriamo ad esempio S: di nuovo il dominio sarebbe tutto $\mathbf{U}$ e quindi S *non è una funzione* in senso insiemistico. Parleremo allora di 'costruzione (insiemistica)' nel caso del successore, dell'unione, ...

- Lo stesso vale per altri simboli da definire in séguito. Comunque useremo liberamente i simboli già definiti, spesso anche abbreviandoli o sostituendoli con espressioni italiane per maggior chiarezza.

2.2.3 Potenze, prodotti cartesiani

L'introduzione dell'insieme delle parti permette di riottenere il fondamentale teorema di Cantor sulla potenza 1.2.17 e nuove costruzioni insiemistiche, ad esempio quelle di prodotto cartesiano e di insiemi di funzioni. Anzitutto, si noti che

$$x \in a \wedge y \in b \Rightarrow \{x\},\ \{x;y\} \in \mathcal{P}(a \cup b) \Rightarrow (x;y) \in \mathcal{P}(\mathcal{P}(a \cup b))$$

Dunque si può definire, usando un assioma di specificazione, il prodotto cartesiano di due insiemi:

Definizione 2.2.13. Il prodotto cartesiano di due insiemi a e b è

$$a \times b = \{z \in \mathcal{P}(\mathcal{P}(a \cup b)); \exists x \in a\, \exists y \in b\ z = (x;y)\}$$

Se quindi R è una relazione per cui $dom(R) \subseteq a$ e $Im(R) \subseteq b$ risulta $R \subseteq a \times b$: di solito una relazione (o una funzione) vengono quindi definite come sottoinsiemi di un prodotto cartesiano, ma questo come si vede non è indispensabile: anzi, complica le definizioni seguenti. L'insieme delle funzioni con dominio a e codominio b si può ora definire con

Definizione 2.2.14.

$$F(a;b) = \{f \in \mathcal{P}(a \times b); f \text{ è una funzione di dominio } a \text{ e codominio } b\}$$

Quindi sono insiemi le collezioni di corrispondenze iniettive o biunivoche tra a e b, eccetera.

È possibile introdurre ora il prodotto cartesiano di una famiglia di insiemi, ma ciò richiede preliminarmente una identificazione del prodotto $a \times b$ già definito con un altro insieme.

Osservazioni 2.2.15.

- Si può identificare la coppia $c = (x_1; x_2) \in a_1 \times a_2$ con la funzione $f_c : \{1; 2\} \to a_1 \cup a_2$, $f_c(k) = x_k,\ k = 1, 2$. Il prodotto cartesiano $a_1 \times a_2$ risulta allora (identificabile con) il sottoinsieme di $F(\{1; 2\}; a_1 \cup a_2)$ delle funzioni f tali che $f(k) \in a_k,\ k = 1, 2$.
- Questo procedimento si estende immediatamente a prodotti cartesiani di un numero finito $n > 2$ di insiemi $a_1, a_2, \ldots, a_n$ considerando le n-uple come funzioni $f : \{1; 2; \ldots; n\} \to \cup_{k=1}^{n} a_k$ tali che $f(k) \in a_k$ per ogni $k = 1, 2, \ldots, n$. Naturalmente, si può definire $a_1 \times a_2 \ldots \times a_n$ semplicemente come l'insieme delle n-uple $(x_1; x_2; \ldots; x_n)$ con $x_k \in a_k$ per ogni $k = 1, \ldots, n$: ma la precedente costruzione, identificabile con questa, si può generalizzare a insiemi qualsiasi di indici.

Definizione 2.2.16. Il prodotto cartesiano di una famiglia a di insiemi (simbolo: $\prod a$) è l'insieme delle funzioni $f : a \to \cup a$ tali che $f(x) \in x$ per ogni $x \in a$. Se la famiglia è indicizzata da $g : b \overset{su}{\to} a$ e $g(x)$ si indica con a_x $(x \in b,\ a_x \in a)$, il prodotto si indica con $\prod_{x \in b} a_x$, e così via.

Se $\emptyset \in a$ si ha ovviamente $\prod a = \emptyset$.

Se si usano prodotti cartesiani si possono anche definire inverse di relazioni e funzioni:

Definizione 2.2.17.

- L'inversa R^{inv} di una relazione R è

$$R^{inv} = \{z \in Im(R) \times dom(R); z = (b; a) \wedge (a; b) \in R\}$$

- Una funzione $f : A \longrightarrow B$ è sempre invertibile come relazione: se l'inversa relazionale f^{inv} è una funzione si pone $f^{inv} = f^{-1}$ (*funzione* inversa di f) e si dice che f è invertibile. Tuttavia, l'uso comune, che seguiremo, indica con f^{-1} anziché con f^{inv} le *controimmagini* di insiemi e punti: $f^{-1}[b] = \{x \in A;\ f(x) \in b\}$, $f^{-1}[y] = \{x \in A;\ f(x) = y\}$.

Si provano i soliti risultati a questo proposito: ad esempio, per una funzione essere invertibile equivale a essere iniettiva.

Analogamente, si può definire la composizione di relazioni (e in generale di insiemi) molto più in generale, ma di solito essa viene considerata soltanto per funzioni:

Definizione 2.2.18. La composizione di due funzioni f e g è la funzione $x \mapsto f(g(x))$ —definita soltanto per gli $x \in dom(g)$ per cui ciò ha senso ($g(x) \in dom(f)$). Essa viene solitamente indicata con $f \circ g$ o semplicemente con fg. Come insieme di coppie $f \circ g$ risulta essere

$$\{z \in dom(g) \times Im(f);\ \exists x \exists w (z = (x; w) \wedge \exists u \in dom(f)(u = g(x) \wedge w = f(u)))\}$$

2.3 Lo schema di rimpiazzamento

Resta da parlare di uno schema che trova spesso applicazione nella teoria, ma che è raramente usato nella matematica corrente: lo *schema di rimpiazzamento*, specificamente dovuto a Fraenkel. L'idea intuitiva che porta allo schema è assai semplice: se si rimpiazzano gli elementi di un insieme con altri si ottiene un nuovo insieme. Come esprimerla formalmente? Ritorniamo alla definizione di simboli funzionali, come ad esempio il successore: lo schema dirà sostanzialmente che se restringiamo una simile costruzione a un dominio che sia un insieme, otteniamo una 'vera' funzione. Fraenkel notò che questo non è garantito nel caso generale da altri assiomi, mentre ciò risulta indispensabile per lo sviluppo della teoria cantoriana. Naturalmente, come sempre per definire un simbolo funzionale, ci vuole un risultato di unicità.

Per comodità esprimeremo questo assioma in forma più generale, permettendo che la funzione non sia ovunque definita: seguiamo [Abian 1972, Cap.II, §4] [3] . Precisiamo meglio e vediamo cosa si intende per una fbf funzionale su un insieme a:

Definizione 2.3.1. $\phi = \phi(v; w)$ sia una fbf nelle due variabili esplicitate, più eventualmente altre (*parametri*): essa è funzionale in v su a se

$$\forall v \in a \forall w_1 \forall w_2 (\phi(v; w_1) \wedge \phi(v; w_2) \Rightarrow w_1 = w_2)$$

In altre parole, dato $v \in a$, se esiste un w tale che $\phi(v; w)$, esso è unico.

Per ϕ di questo tipo, lo schema esprime ora il fatto che, se 'rimpiazziamo' quegli $x \in a$ per cui vale $\phi(x; w)$ con l'unico w possibile, si ottiene un altro insieme.

Schema di rimpiazzamento [R] Dati un insieme a e una fbf $\phi = \phi(x; y)$, funzionale in x su a, esiste l'insieme $b = \{z;\ \exists x \in a\, \phi(x; z)\}$
$\forall v_0[(\forall v_1 \in v_0 \forall w_1 \forall w_2 (\phi(v_1; w_1) \wedge \phi(v_1; w_2) \Rightarrow w_1 = w_2)) \Longrightarrow$ $\Longrightarrow (\exists v_2 \forall v_3 (v_3 \in v_2 \Leftrightarrow \exists v_1 (v_1 \in v_0 \wedge \phi(v_1; v_3))))]$

Osservazioni 2.3.2.

1. ϕ può avere altre differenti variabili libere oltre a quelle esplicitate, ma non v_2 (che indica l'insieme b): come sempre in questo caso si premettono le relative quantificazioni universali affinché gli assiomi siano enunciati.

2. Spesso lo schema viene enunciato con la condizione di funzionalità

$$\forall x \in a \exists!\, z\, \phi(x; z)$$

e postulando l'esistenza di un insieme c che ha fra gli elementi quelli di b: in questo modo lo schema modificato (chiamiamolo R') afferma, in maniera più trasparente, il fatto che $\phi(v; w)$ determina una funzione *di dominio a*. La ragione della generalizzazione di R' in R risiede in un criterio di economia: di fatto, così formulato, lo schema R rende superflui lo schema S e l'assioma C; qui li si è enunciati per una descrizione più piana delle costruzioni insiemistiche, anticipando quelle

[3] Lo schema viene lì chiamato 'di sostituzione'.

più semplici (gli assiomi di R non vengono in genere compresi tra gli assiomi 'elementari').

3. Di fatto, lo schema S viene ottenuto, per un insieme a e una fbf ψ, mediante lo schema R, se ϕ è data dalla fbf, funzionale in z su a, $w = z \wedge \psi(z)$: in effetti

$$\{z \in a;\ \psi(z)\} = \{w; \exists z \in a(w = z \wedge \psi(z))\};$$

naturalmente l'assioma E di estensione è richiesto per avere una definizione ben posta.

4. Inversamente, lo schema R' viene facilmente ottenuto da R (da E —e da S che ne è però una conseguenza), dal momento che $\exists z\phi(x; z)$ determina un sottoinsieme degli $x \in a$ per S e ad esso è applicabile la richiesta di *esistenza* e unicità del n.2. In effetti, R' è un caso particolare di R.

5. Inoltre, l'assioma C si ottiene da E, R, P considerando $\mathcal{P}(\mathcal{P}(\emptyset)) = = \{\emptyset;\ \{\emptyset\}\}$: da esso per rimpiazzamento si ottiene $\{a;\ b\}$ per ogni a, b, cioè C.

6. Dato che lo schema determina una funzione f di dominio a (per semplicità) e immagine b mediante la formula ϕ, b stesso viene in genere descritto come $\{f(x); x \in a\}$. Poiché in genere si parte da una definizione di funzione dando direttamente gli insiemi dominio d e codominio c, e quindi f come sottoinsieme di $d \times c$, l'assioma non è adoperato correntemente, ma è indispensabile nella teoria dei numeri cardinali e ordinali. Vedi l'esempio 2.4.4 sotto e il capitolo 4.

7. In qualche senso, questo schema R è più elementare dell'assioma della potenza P, per cui a volte lo si introduce prima di P: con esso e C, ma senza P, e quindi senza la nozione di prodotto cartesiano, è possibile definire molte costruzioni, come l'inversa di una relazione R (rimpiazzamento di ogni $(x; y) \in R$ con $(y; x)$) o la composizione di funzioni f e g.

Esercizio 2.3.3. Perché con E, S, C, ma senza lo schema di rimpiazzamento, si deve usare l'assioma della potenza per definire $f \circ g$ come si è fatto prima?

2.3.1 La consistenza della teoria generale degli insiemi

Gli assiomi fin qui enunciati (E, S, C, U, P, R o anche soltanto E, U, P, R) formano una teoria generale degli insiemi (TGI) di cui è facile provare la consistenza, se si ammette l'uso intuitivo di $\mathbb{N}$, ma anche l'inadeguatezza a formalizzare la matematica.
Costruiremo ora un modello per questi assiomi, usando appunto i numeri naturali [Abian 1972, Cap.II, §5]. A causa dell'unicità della loro rappresentazione binaria (A.2), *ogni numero naturale è somma di potenze di due con esponenti diversi in un unico modo, a parte l'ordine di presentazione.* Interpretiamo allora il linguaggio insiemistico in una struttura $\mathfrak{I} = (\mathbb{N}; \in^{\mathfrak{I}})$ in modo che la relazione $\in^{\mathfrak{I}}$ sia la relazione esponente-numero nella rappresentazione binaria; l'uguaglianza al solito è interpretata come identità. Ad esempio, $13 = 2^3 + 2^2 + 2^0$ e quindi gli 'elementi' dell''insieme' 13 sono 0,2,3. Si verifica facilmente che E vale, e quindi possiamo scrivere $13 = \{0; 2; 3\}^{\mathfrak{I}}$. Analogamente $0 = \emptyset^{\mathfrak{I}}$, giacché 0 è l'unico numero 'senza esponenti'. $\mathfrak{I}$ è un modello di TGI, come si può verificare [Abian 1972, loc. cit.]. Vediamo ad esempio come esista sempre la coppia non ordinata $\{a; b\}$, lasciando per esercizio il caso $a = b$: consideriamo quindi $a \neq b$. In tal caso $\{a; b\}^{\mathfrak{I}} = 2^a + 2^b$. Identifichiamo, se non porta a confusione, gli insiemi a, b coi relativi numeri naturali per semplicità.

Esercizi 2.3.4.

1. Nel modello $\mathfrak{I}$, quale è l'interpretazione del singoletto $\{a\}$? E quella di $\{\{\emptyset\}\}$?
2. Analogamente, quale è l'interpretazione del successore (definizione 2.2.10) di a?

Giacché esiste questo modello per TGI, essa è consistente; inoltre si può provare con modelli elementari che i quattro assiomi [4] E, R, P, U sono in-

[4] Più esattamente, tre assiomi e uno schema.

dipendenti, ognuno dagli altri tre; per una analisi più approfondita, vedi [Abian 1972, Cap.II, §6]. Anche questa è una motivazione per enunciare R come si è fatto.

Però se si osserva che tutti gli insiemi in $\mathfrak{I}$ sono finiti, è intuitivamente chiaro che:

in TGI non si può dimostrare l'esistenza di insiemi infiniti.

Per la matematica, gli insiemi infiniti sono essenziali: risulta quindi necessario un assioma apposito di esistenza, indipndente dai precedenti.

2.4 L'assioma dell'infinito

Questo assioma è dato nello stile dei precedenti C, U, P: si garantisce tramite l'esistenza di un insieme c quella di uno specifico insieme infinito, anzi della controparte formale di $\mathbb{N}$. Premettiamo una definizione.

Definizione 2.4.1. Un insieme c è induttivo quando

(i) $\emptyset \in c$;

(ii) se $x \in c$, allora anche $Sx \in c$.

Abbreviamo questa proprietà con Ind.

L'assioma è allora semplice da enunciare:

Assioma dell'infinito [I]
Esiste un insieme induttivo
$\exists v_0(\emptyset \in v_0 \wedge (\forall v_1 \in v_0\ Sv_1 \in v_0))$, cioè $\exists v_0(Ind(v_0))$

L'assioma assicura che la classe **Ind** non è vuota; dunque è ben definita l'intersezione $\bigcap_{Ind(x)} x$ di tutti gli insiemi induttivi, che è a sua volta induttiva: è il minimo insieme induttivo, che viene indicato con ω.

Definizione 2.4.2.

$$\omega = \bigcap_{Ind(x)} x$$

Osservazioni 2.4.3.

- ω contiene i numerali di von Neumann: è il rappresentante insiemistico di $\mathbb{N}$. In particolare, si noti che il principio di induzione è immediato per la minimalità di ω tra gli insiemi induttivi: se $a \subseteq \omega$ è induttivo, si ha subito $a = \omega$.

- Un insieme è numerabile se esiste una corrispondenza biunivoca con ω.

- Chiamiamo *numeri naturali* i suoi elementi: è questa una definizione indiretta, ma che potrebbe permettere di ricavare le loro proprietà usuali (quelle derivanti da PA), sebbene non sempre facilmente: si noti quali di queste sono necessarie nel séguito e si tenti di dimostrarle. Per ora procediamo dandole sostanzialmente per acquisite: più avanti daremo dei naturali come insiemi una definizione diretta (la definizione 4.2.7) che permette di ricavarle agevolmente.

- Altre proprietà dei numeri naturali sono incidentali e, per quanto bizzarre rispetto alla nozione ordinaria, sono strumentali e assai comode per sviluppare l'aritmetica nell'àmbito di ZF: ci si riferisce al fatto che un numero naturale è *elemento* (e anche sottoinsieme) dei numeri maggiori di esso, e simili. Anche queste proprietà potrebbero venir provate dalla precedente definizione di ω, ma sono più semplici da dimostrare con la definizione esplicita a cui si è già accennato.

Limitatamente ad ω dunque valgono gli assiomi di PA, relativizzati ad esso: indichiamoli con PA_ω [5] ($ZF \vdash PA_\omega$); in particolare si vedrà (in 4.2.7) che si ritrova la relazione d'ordine, con la fondamentale proprietà di minimo, ma *rappresentata da* $\in$: $m < n \Leftrightarrow m \in n$. Come conseguenza inevitabile, è ora impossibile provare la consistenza di $ZF^- = \{E; S; C; U; P; R; I\}$ [6] . Ma

[5] Per questa parte, vedi *Appunti sulla ricorsività*, sezione 6.2.

[6] Si noti però che —senza R— E, P, U, I sono consistenti: [Abian 1972, Cap.II, §8, Proposizione 16].

non è neanche possibile riprodurre i paradossi classici, che diventano prove per assurdo in ZF^- dell'esistenza di classi proprie: la classe universale, la classe di Russell,...

Per contro, si può ora inquadrare l'intera matematica classica entro la teoria degli insiemi, dato che si possono costruire, con metodi giustificati dagli assiomi, le strutture numeriche $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, gli insiemi di funzioni $F(\mathbb{R};\mathbb{R})$, e in séguito gli insiemi delle funzioni continue $\mathbb{R} \to \mathbb{R}$, eccetera. Infine, possiamo ora mostrare usando I un esempio di insieme la cui esistenza è giustificabile soltanto con lo schema di rimpiazzamento.

Esempio 2.4.4. Si consideri una successione definita 'per ricorrenza' da

$$\mathcal{P}_n(\omega) = \begin{cases} \omega & \text{se} \quad n = 0 \\ \mathcal{P}(\mathcal{P}_{n-1}(\omega)) & \text{se} \quad n > 0 \end{cases}$$

Si può verificare che per ogni $n \in \omega$ $\mathcal{P}_n(\omega)$ è ben definito [7] : quindi, per rimpiazzamento è un insieme $\{\mathcal{P}_n(\omega); n \in \omega\}$ e lo è dunque $\Omega = \bigcup_{n=0}^{\infty} \mathcal{P}_n(\omega)$. Questo è un esempio di un insieme di potenza a stento immaginabile, dato che gli insiemi della successione hanno potenza sempre crescente, a partire dal numerabile, e quindi Ω ha potenza superiore a tutti questi (teorema di Cantor 1.2.17).

Come si può intuire dal simbolo ZF^-, non abbiamo terminato di esporre il sistema d'assiomi correntemente designato con ZF: per completarlo, nel prossimo capitolo (sezione 3.1) vedremo un ultimo assioma, che però, curiosamente, non ha applicazioni in matematica. Soltanto la sua rilevanza per l'idea intuitiva di insieme e, soprattutto, la descrizione particolarmente limpida che esso permette dell'universo insiemistico (cap.4) ne consigliano l'inclusione nel sistema canonico di Zermelo-Fraenkel.

[7] Si usa il principio di induzione ordinario, giustifcabile in PA; vedi anche il caso dell'induzione transfinita, teorema 4.2.14.

Capitolo 3

Assiomi speciali: ZFC e ampliamenti

Gli assiomi visti finora possono bastare allo sviluppo di una teoria elementare generale sufficiente all'inquadramento della matematica classica, ma per ottenere risultati più profondi o per studiare le capacità e i limiti di ZF^- si è rivelato necessario introdurre ulteriori assiomi, di interesse per i fondamenti (l'assioma, appunto, di fondazione) o di grande utilità specificamente matematica (l'assioma di scelta). Trattiamo ora di questi due assiomi e dei problemi connessi.

3.1 Gli assiomi di regolarità e di fondazione

Sembra una nozione del tutto ovvia che un insieme non possa appartenere a se stesso come elemento; stranamente, questo enunciato ($\forall v_0(v_0 \notin v_0)$) non è derivabile a partire dagli assiomi visti. Dopo varie proposte per ovviare a questa apparente incongruenza della teoria, fu introdotto un assioma (*di fondazione*: FA [1]) apposito, che attualmente viene presentato in una forma forte, come *assioma di regolarità* (Reg), 'quasi' equivalente al primo (sezione

[1]Noto talvolta col suo nome originale tedesco: *Fundierungsaxiom*.

3.2); esso permette di chiarire la gerarchia di complessità costruttiva degli insiemi (ora nota come *gerarchia di von Neumann*: capitolo 4, pagina 82).

Vediamo anzitutto due definizioni.

Definizioni 3.1.1.
1. Un insieme a è ben fondato se non esiste una successione $\in$-*discendente* in esso, cioè una successione $(a_m)_{m=0}^{\infty}$ tale che $\ldots \in a_{n+1} \in a_n \in a_{n-1} \in \ldots \in a_2 \in a_1 \in a_0 = a$. Abbreviamo questa proprietà con $WF(a)$ (WF sta per *well founded*, 'ben fondato').

2. Un insieme a è regolare se $a = \emptyset$ oppure $\exists b(b \in a \wedge a \cap b = \emptyset)$. A parole: a è regolare se è vuoto, oppure se contiene un elemento disgiunto da esso. Abbreviamo questa proprietà con $Reg(a)$.

È ora facile enunciare i due assiomi detti:

Assioma di fondazione [FA]	**Assioma di regolarità [Reg]**
Ogni insieme è ben fondato	Ogni insieme è regolare
$\forall v_0 WF(v_0)$	$\forall v_0 Reg(v_0)$

FA ha per conseguenza immediata l'impossibilità di $\in$-cicli del tipo $a \in a$ e anche $a_0 \in a_1 \in \ldots \in a_n \in a_0$, venendo incontro alle esigenze dell'intuizione, ma attualmente è visto come una conseguenza dell'assioma di regolarità.

Teorema 3.1.2. *$ZF^- \vdash Reg \Rightarrow FA$. In altri termini: in ZF^-, l'assioma di regolarità implica quello di fondazione.*

Dimostrazione. Ragioniamo (informalmente) per contrapposizione: supponiamo che FA non valga e a non sia ben fondato, a causa della $\in$-successione $\sigma = (a_m)_{m=0}^{\infty}$. Dato che le successioni sono funzioni, possiamo considerare come dato l'insieme $b = \{a_m;\ m \in \omega\} = Im(\sigma)$: esso non è regolare. Infatti, dato un suo elemento a_j qualunque, si ha sùbito $a_{j+1} \in a_j \cap b \neq \emptyset$.
Dunque Reg non vale. $\square$

Di fatto, l'esistenza di insiemi a per cui $a \in a$ non è refutabile in ZF^- e quindi non porta a risultati contraddittori, seppure si abbiano conseguenze paradossali, ma solo perché contrastanti con l'idea corrente di insieme.

Sebbene non abbia particolari applicazioni in matematica, Reg per le sue conseguenze è spesso considerato parte integrante dell'idea di insieme e perciò viene incorporato in ZF: denotiamo quindi infine con ZF gli assiomi di $ZF^{-} \cup \{Reg\} = \{E; S; C; U; P; R; I; Reg\}$.

Reg, oltre a impedire la stranezza $x \in x$ per qualche insieme autoreferenziale, permette, come si è detto, una costruzione assai elegante della totalità degli insiemi (pag.82). D'altra parte, gli insiemi di cui si serve la matematica possono essere comunque ben fondati, e quindi la questione della esistenza di insiemi non ben fondati è "essenzialmente irrilevante" [Kunen 1980].

Si sono però notati casi in cui nella modellizzazione matematica potrebbe essere utile avere a che fare con insiemi del genere, ma in maniera controllabile: diversi costrutti (ad esempio nel campo dell'informatica) presentano fenomeni di circolarità che mal si prestano ad essere schematizzati con naturalezza mediante insiemi ben fondati. Per questi problemi si è proposta l'introduzione di certi insiemi non regolari (*iperinsiemi*): vedi [Barwise-Moss 1991] per una esposizione divulgativa di un assioma di 'antifondazione' (P. Aczel, 1988).

3.2 L'assioma di scelta

Questo assioma formalizza un principio liberamente usato già da Cantor, ma criticato da altri matematici dell'epoca (Peano, Poincaré) per il suo carattere altamente non costruttivo, quando viene assunto nella sua più completa generalità. Esso deve il suo nome al fatto che si postula di poter sempre effettuare un numero anche infinito di scelte simultanee di un elemento da ciascun insieme di una qualunque famiglia, senza che si possa in alcun modo specificare un particolare algoritmo di scelta.

Assioma di scelta [AS] Data una famiglia $a \neq \emptyset$ di insiemi non vuoti, esiste sempre una $f : a \to \cup a$ tale che $f(x) \in x$ per ogni $x \in a$
$\forall v_0[(v_0 \not\equiv \emptyset \wedge \forall v_1 \in v_0(v_1 \not\equiv \emptyset)) \Rightarrow (\exists v_2 \in F(v_0; \cup v_0)\forall v_1 \in v_0(v_2(v_1) \in v_1)]$

La storia di questo assioma, assai complessa, è stata ricostruita magistralmente in [Moore 1982], che contiene il materiale che verrà citato di séguito e moltissimo altro. A grandi linee, si può dire che, mentre per molti secoli i matematici hanno inteso come necessaria in una dimostrazione di esistenza una 'costruzione', un procedimento più o meno dettagliato che si potesse eseguire —almeno in linea di principio— per ottenere un esempio esplicito, cominciarono a presentarsi nel XIX secolo situazioni in cui, per la grande generalità, non era importante descrivere una costruzione nei dettagli, e la si postulava. Tipico il caso della seguente, elementare affermazione di topologia della retta reale.

Proposizione 3.2.1. *Un $x_0 \in \mathbb{R}$ è di accumulazione per un sottoinsieme A di $\mathbb{R}$ se e solo se esiste una successione di elementi di A, tutti diversi da x_0, convergente ad x_0.*

Si intende che, per definizione, x_0 è di accumulazione per A se e solo se in ogni intorno di x_0 cadono infiniti punti di A. La dimostrazione consiste essenzialmente nello *scegliere* un $x_n \in A$ diverso da x_0 in ogni intervallo $[x_0 - \frac{1}{n}; x_0 + \frac{1}{n}]$: ma come è possibile specificare un algoritmo di scelta del tutto generale? Si ammetteva di poter effettuare la costruzione sulla scorta degli esempi più semplici: ma in effetti veniva impiegato un nuovo principio, non costruttivo. Forse il primo matematico a intuire che veniva implicitamente usata una nuova assunzione fu G. PEANO; in un suo lavoro del 1890, sull'esistenza di soluzioni per sistemi di equazioni differenziali ordinarie, si trovò a dover effettuare una scelta per ogni insieme di una successione, e osservò[2] (trad. dall'originale in francese):

> [Poiché] non si può applicare una infinità di volte una regola *arbitraria* con la quale assegnare a una classe a un membro di questa classe, si determina qui una *ben precisa* regola per mezzo della quale a ogni classe a, sotto opportune ipotesi, si assegna un membro di questa classe[...]

[2]G. Peano: 'Démonstration de l'intégrabilité des équations différentielles ordinaires', *Mathematische Annalen*, Bd. XXXVII A.1890, pp. 182-228, in *Opere Scelte, vol.I, p.150.*

Negli anni seguenti, furono sollevate poche osservazioni al proposito, tranne quelle di alcuni matematici italiani (R. Bettazzi, B. Levi). Chi per primo propose esplicitamente l'assioma fu Zermelo, che lo impiegò nella dimostrazione del suo teorema del buon ordinamento che Cantor stesso, il quale pure aveva impiegato più volte implicitamente il principio delle scelte, non era riuscito a provare, sebbene rivestisse una importanza cruciale per la teoria dei numeri cardinali (vedi sezione 4.3).

3.2.1 Proposizioni equivalenti ad AS

Il teorema di Zermelo fu il primo di molti enunciati che verranno provati equivalenti in ZF all'assioma, nei campi più svariati della matematica. Vediamone l'enunciato (per la definizione di buon ordinamento, vedi l'appendice A.3.1).

Teorema 3.2.2. ***(di Zermelo, del buon ordinamento, 1904)*** *Ogni insieme è bene ordinabile.*

Per una dimostrazione, vedi [Abian 1972, cap. IV, §6, teorema 41]. □
A differenza della dimostrazione originale, quella citata usa un'altra delle proposizioni equivalenti all'assioma, il cosiddetto lemma di Zorn, molto usato in algebra al posto di AS:

Teorema 3.2.3. ***(Lemma di Zorn, 1935)*** *Se $A \neq \emptyset$ è una famiglia di insiemi debolmente ordinata da subseteq e ogni suo sottoinsieme totalmente ordinato non vuoto è superiormente limitato, esiste un elemento massimale in A rispetto all'inclusione.*

È equivalente il caso di un insieme A debolmente ordinato da una relazione R qualsiasi. Per una dimostrazione, vedi [Abian 1972, loc. cit., teorema 39]. □
Il lemma di Zorn è solo il più sfruttato tra numerosi enunciati equivalenti ad AS concernenti elementi massimali, specie rispetto all'inclusione (i cosiddetti *principi di massimalità*): vedi [Moore 1982, 4.4] o [Smullyan-Fitting 1996, cap.4, §5].

Vi sono poi formulazioni equivalenti, assai semplici, ma non meno utili.

Teorema 3.2.4. *Sono equivalenti (in ZF) le seguenti proposizioni:*

1. *l'assioma di scelta;*

2. *l'assioma di scelta per famiglie di insiemi disgiunti;*

3. ***Assioma di selezione**. Data una partizione $\mathcal{G}$ di un insieme $A \neq \emptyset$ (o, che è lo stesso, una relazione di equivalenza su A), esiste un sottoinsieme $B \subseteq A$ che interseca ogni insieme della partizione esattamente in un punto. B si dice un* insieme di selezione *per $\mathcal{G}$, o per l'associata relazione di equivalenza;*

4. *data una qualunque funzione f, esiste una sua restrizione $g \subseteq f$ iniettiva e con la stessa immagine;*

5. *data una qualunque funzione $f : a \xrightarrow{su} b$, esiste una funzione iniettiva $h : b \longrightarrow a$ tale che $f(h(x)) = x$ per ogni $x \in b$;*

6. *data una qualunque relazione R, esiste una funzione $g \subseteq R$ con lo stesso dominio.*

Dimostrazione.

- 2 è un caso particolare di 1;

- 2 implica 3. Se f è una funzione di scelta per $\mathcal{G}$, dato che si tratta di una famiglia non vuota di insiemi non vuoti e disgiunti, $B = Im(f)$ è un insieme di selezione per $\mathcal{G}$;

- 3 implica 4. Se $f : a \to b$, si consideri $\mathcal{G} = \{f^{-1}(y);\ y \in Im(f)\}$: questa è una partizione di a; per 3, esiste un insieme di selezione $c \subseteq a$ per $\mathcal{G}$. Dunque se si restringe f a c si ha una funzione iniettiva $g : c \to b$ con immagine $Im(f)$.

- 4 implica 5. Nella ipotesi 4, la funzione iniettiva g ottenuta nel passo precedente ha immagine b: allora la sua inversa g^{-1} ha dominio b e $(f \circ g^{-1})(x) = x$, dal momento che g è una restrizione di f: si ponga quindi $h = g^{-1}$.

- 5 implica 6. Si considerino la proiezione [3] $P_1 : R \xrightarrow{su} dom(R)$ e la funzione $H : dom(R) \xrightarrow{1-1} R$, la cui esistenza è assicurata da 5. Se $H(x) = (x; y)$, xRy e quindi $P_2 \circ H$, dove P_2 è la proiezione sulla seconda componente delle coppie $(x; y) \in R$, è la funzione cercata.

- 6 implica 1. Se $a \neq \emptyset$ è la famiglia di insiemi non vuoti per cui si cerca una funzione di scelta, si consideri la relazione $R \subseteq a \times \bigcup a$ definita da

$$xRy \iff x \in a \wedge y \in \bigcup_{x \in a} x \wedge y \in x.$$

Per 6, esiste una funzione $f : a \longrightarrow \bigcup a$ tale che, per ogni $x \in a$, $xRf(x)$, cioè $f(x) \in x$. $\square$

Numerose altre proposizioni sono equivalenti all'assioma, in teoria degli insiemi, topologia, algebra e logica [Moore 1982, App.2, table 9]. Citiamo gli enunciati di questi tre importanti risultati equivalenti ad AS:

- l'assioma moltiplicativo;

- il teorema di Löwenheim-Skolem(-Tarski);

- il teorema di compattezza di Tychonoff.

senza dare tutti i dettagli delle definizioni conivolte, e tanto meno le dimostrazioni.

Teorema 3.2.5. ***(Assioma moltiplicativo, di Russell)*** *Se $a \neq \emptyset$ è una famiglia di insiemi non vuoti, allora $\prod a \neq \emptyset$.*

[3]Ovviamente, $P_1 : (x; y) \mapsto x$ e in séguito $P_2 : (x; y) \mapsto y$ sono funzioni di dominio R.

In questo caso la dimostrazione dell'equivalenza è immediata, trattandosi di una mera riformulazione di AS, fondata sulla definizione generale 2.2.16 di $\prod a$, già vista.

Teorema 3.2.6. ***(Teorema di Löwenheim-Skolem-Tarski)*** *Ogni insieme di enunciati che abbia un modello (normale) infinito, ne ha uno di qualunque cardinalità infinita.*

Dimostrazione in [Ebbinghaus-Flum-Thomas 1994, chapt.VI, 2.4].

Teorema 3.2.7. ***(Tychonoff)*** [4] *Il prodotto di qualunque famiglia di spazi topologici compatti è compatto.*

3.2.2 Conseguenze paradossali di AS

AS dà luogo a controesempi e veri e propri paradossi in molti campi della matematica: questo lo ha fatto considerare con sospetto, come una potenziale fonte di contraddizioni in ZF. Citiamo due esempi notevoli.

Proposizione 3.2.8. ***(Vitali, 1905)*** *Esistono sottoinsiemi $A \subset \mathbb{R}$ non misurabili nel senso di Lebesgue.*

Di più, furono ottenuti con AS una gran varietà di insiemi non misurabili [5]: ogni intervallo di $\mathbb{R}$ ne contiene, e anche ogni intervallo di $\mathbb{R}^n$. Da AS segue che [Moore 1982, 2.3]

- non esiste alcuna estensione della misura di Lebesgue invariante per traslazione che sia definita su tutti i sottoinsiemi di $\mathbb{R}$; inoltre
- i sottoinsiemi misurabili di $\mathbb{R}$ costituiscono una famiglia con la potenza 'soltanto' del continuo.

Questo esempio è paradossale anche perché un tale insieme ha la proprietà di essere misurabile soltanto 'dall'esterno', in modo da risultare divisibile in due parti disgiunte di misura esterna complessiva strettamente maggiore di

[4] Vedi anche J.L. Kelley, General Topology, Van Nostrand, New York etc. 1955: 5.13.

quella di partenza. Questa proprietà controintuitiva giunge quasi all'assurdo con il seguente paradosso:

Proposizione 3.2.9. ***(Banach e Tarski, 1924)*** *Se $S_r \subset \mathbb{R}^3$ è una qualsiasi sfera (solida) di raggio r nello spazio euclideo ordinario, è possibile suddividerla in un numero finito di parti riassemblabili (con movimenti rigidi) in* due *sfere complete con lo stesso raggio r!*

Iterando il procedimento, da una sfera se ne possono ottenere quante se vogliano (in numero finito) per decomposizione in un numero finito di parti disgiunte —evidentemente non misurabili— e movimenti rigidi. Si può provare addirittura che in $\mathbb{R}^n$, se $n \geq 3$, due insiemi limitati qualsiasi con interno non vuoto sono equivalenti per decomposizione in parti finite congruenti (originario risultato di Banach e Tarski: vedi [Moore 1982, 4.11]).

3.2.3 Risultati dipendenti da AS

Alcune delle conseguenze più significative di AS sono legate al rapporto, apparentemente di semplice negazione, tra insiemi finiti e insiemi infiniti. Questa distinzione sembra indipendente da AS, dal momento che l'esistenza di una funzione di scelta nel caso di una famiglia finita di insiemi può essere *provata* in ZF; al contrario, l'assioma risulta indispensabile per distinguere nettamente il finito dall'infinito.

AS e il finito

Finora abbiamo usato una nozione intuitiva di finito, ma potrebbe sembrare che una definizione soddisfacente derivi dalla negazione della proprietà indicata da Dedekind per caratterizzare gli insiemi infiniti (vedi la definizione 1.2.1). Chiamiamo provvisoriamente questa definizione 'di non-infinitezza' (il nome più diffuso è 'D-finitezza', 'finitezza secondo Dedekind'):

Definizione 3.2.10. Un insieme A è non-infinito (D-finito) se *non* può essere messo in corrispondenza biunivoca con alcuna sua parte propria.

Tuttavia, la definizione più spontanea di insieme finito sarebbe: un insieme è finito se è vuoto, o lo si può mettere in corrispondenza biunivoca con $\{1; \ldots ; n\}$ per un qualche numero naturale n. Un enunciato preciso del genere risale nella sostanza a R. Bettazzi, allievo di Peano, che rese rigorosa, sia pure in àmbito non ancora insiemistico, la intuizione alla base della parola stessa (vedi [Moore 1982]). Come si vede, la nozione di finito è strettamente collegata ai numeri naturali; con essi è possibile dare una definizione più concisa, che attribuiremo sempre a Bettazzi:

Definizione 3.2.11. (R. Bettazzi, 1896) Un insieme è finito se può essere messo in corrispondenza biunivoca con qualche numero naturale $j \in \omega$.

Ora, si desidererebbe che queste due definizioni di finito fossero equivalenti: piuttosto strano risulta il fatto che è possibile ottenere ciò soltanto usando AS.

Per capire meglio il problema, iniziamo con l'esaminare in dettaglio alcune conseguenze della definizione precedente. A questo scopo, daremo ancora per acquisite diverse proprietà degli elementi di ω —ad esempio che si tratti di insiemi con particolari proprietà, che il successivo insiemistico abbia in ω le consuete proprietà, eccetera, che sono sì dimostrabili (vedi [Abian 1972, Cap.II, §8]), ma che si possono provare più agevolmente considerando i numeri naturali come particolari *numeri ordinali*: vedi 4.2. Con questi presupposti proviamo anzitutto che

Teorema 3.2.12. *Nessun $j \in \omega$ può essere messo in corrispondenza biunivoca con una sua parte (sottoinsieme) propria.*

Dimostrazione. Proviamo il teorema per induzione. Il caso $j = 0$ è banale: $\emptyset$ non ha sottoinsiemi propri! Per ipotesi di induzione, l'enunciato valga per un $j = m$ e proviamolo per assurdo nel caso Sm: dunque, esista $A \subset Sm = m \cup \{m\}$ tale che $A \overset{g}{\sim} Sm$ (per il simbolo, vedi appendice A.3.2). Si può supporre $m \notin A$ e quindi $A \subseteq m$: eventualmente si effettua una trasposizione tra m e un $x \notin A$. Se ora $y \in A \mapsto m \in Sm$ tramite g, $B = A \setminus \{y\} \subset m$ è in corrispondenza biunivoca mediante $g \restriction B$ con m, contro l'ipotesi di induzione. □

Poiché ogni $m < n$ è parte propria di n, segue subito

Corollario 3.2.13. *Due numeri naturali m, n diversi non possono essere messi in corrispondenza biunivoca tra loro. Quindi se A è finito, può essere messo in corrispondenza biunivoca con un solo $m \in \omega$: si dice che A è finito con m elementi.*

Risulta ora facilmente che

Teorema 3.2.14. *Se un insieme A è finito, allora è non-infinito (D-finito).*

Dimostrazione. Per assurdo, sia $A \overset{h}{\sim} m$ e anche $B \overset{g}{\sim} A$ con $B \subset A$. Risulta allora $B_0 \sim m$, con $B_0 = h[B] \subset m$, mediante la corrispondenza biunivoca $h \circ g \circ h^{-1}$, contro il teorema precedente. □

Gli insiemi risultano allora ripartiti in linea di principio tra: insiemi finiti, infiniti, e insiemi che non sono finiti, ma nemmeno infiniti (nel senso della definizione 1.2.1). Per analizzare meglio il problema, chiamiamo provvisoriamente 'non-finito' un insieme per cui vale la negazione della definizione 3.2.11. Proviamo anzitutto che

Teorema 3.2.15. *(AS)* [6] *Ogni insieme non-finito ha un sottoinsieme numerabile* [7] *.*

Dimostrazione. Se A è non-finito, si scelgano x_0 in A, poi x_1 in $A \setminus \{x_0\}$, e così via: in generale, scelti $x_0, \ldots, x_m$, x_{m+1} va cercato in $A \setminus \{x_0, \ldots, x_m\}$: l'ipotesi assicura che gli insiemi da cui si estraggono gli x_i non sono mai vuoti. Si verifica facilmente che gli x_i sono a due a due distinti, e quindi A contiene un sottoinsieme numerabile. L'uso di AS non è evidente, ma si potrebbe dimostrare che è essenziale: per scegliere un x_n diverso dai precedenti, occorre una funzione di scelta per $\mathcal{P}(A) \setminus \{\emptyset\}$. □

Questo risultato permette di determinare l'equivalenza tra le due definizioni di finito:

[6] Segnaliamo così la dipendenza del risultato dall'assioma di scelta.

[7] Cioè equipotente ad ω.

Teorema 3.2.16. *(AS) Ogni insieme non-finito è infinito nel senso di Dedekind. Quindi, se un insieme è non-infinito (D-finito), allora è finito.*

Dimostrazione. Se A è non-finito, sia $B \subseteq A$ numerabile, con $B \overset{f}{\sim} \omega$. La funzione $g = f^{-1} \circ S \circ f$ mette in corrispondenza biunivoca B con un suo sottoinsieme proprio (B privato del suo 'primo' elemento $f^{-1}(0)$): prolungando eventualmente g su $A \setminus B$ con l'identità si ottiene una corrispondenza biunivoca di A con una sua parte propria. $\square$
Le due definizioni di finito (e quindi le due di infinito) sono dunque equivalenti, ma solo se vale AS: in effetti il cruciale risultato 3.2.15, che ora si può riformulare come

Un insieme infinito ha sempre sottoinsiemi numerabili

vale soltanto quando vale AS, con le sue successive conseguenze, come ad esempio

Un insieme numerabile ha soltanto sottoinsiemi finiti o numerabili

Esso è comunque fondamentale per la teoria degli insiemi perché delimita con precisione il confine tra finito e infinito insiemistici. Vedremo più avanti che AS permette di confrontare tra loro le infinità di due insiemi qualsiasi.

Nel tentativo di aggirare la difficoltà rappresentata dal necessario uso di AS appena visto, sono state presentate altre definizioni di 'finito', anche per avere criteri intrinseci di finitezza, che non ricorrano all'introduzione, per così dire dall'esterno, dei numeri naturali. Le definizioni seguenti sono interne all'insieme, o, piuttosto, fanno riferimento alla famiglia dei suoi sottoinsiemi. I problemi che si incontrano nel dimostrare l'equivalenza tra queste definizioni e le precedenti sono però gli stessi: l'uso inevitabile dell'assioma di scelta (tipico assioma sull'infinito). Questo sembra indicare che i tradizionali problemi d'esistenza ed i paradossi sull'infinito si possono presentare anche nel finito 'molto grande'.

Citiamo tra le più significative definizioni interne le seguenti due:

Definizione 3.2.17. (Stäckel, 1907). Un insieme è (Stäckel-)finito se e solo se è doppiamente bene ordinabile (cioè ordinabile in modo che ogni suo sottoinsieme non vuoto abbia massimo e minimo). Un insieme è (Stäckel-)*in*finito se e solo se *non* lo si può bene ordinare doppiamente.

Definizione 3.2.18. (Tarski, 1924). Un insieme è (Tarski-)finito se e solo se ogni famiglia non vuota di suoi sottoinsiemi ha un elemento massimale (rispetto all'inclusione). Quindi, un insieme è (Tarski-)*in*finito se e solo se esistono famiglie non vuote di suoi sottoinsiemi senza elemento massimale.

Altre conseguenze notevoli di AS

Iniziamo con una proposizione già menzionata.

Teorema 3.2.19. *(AS) L'assioma di fondazione implica quello di regolarità.*

Dimostrazione. Per contrapposizione, $a = a_0$ sia un insieme non regolare: allora, scelto $b \in a$, $b \cap a$ non è vuoto e quindi si può scegliere $a_1 \in b \cap a$; poiché $a_1 \in a_0$, si può scegliere $a_2 \in a_1 \cap a_0$,... In questo modo si ottiene una successione, definita per induzione, $\ldots, \in a_n \in \ldots \in a_1 \in a_0$, che prova che a_0 non è ben fondato e quindi FA non vale. AS è usato per ottenere una funzione di scelta (la successione degli a_n) nella famiglia di insiemi non vuoti $\{a \cap b;\ b \in a\}$ ottenibile per rimpiazzamento da a. $\square$

Più ampiamente usate sono altre conseguenze dell'assioma: ne menzioniamo qui soltanto un paio, il teorema dell'unione numerabile e il teorema della base per spazi vettoriali.

Anzitutto, ritorniamo sulla proposizione 1.2.6: essa richiede necessariamente qualche forma di scelta.

Teorema 3.2.20. *Unioni al più numerabili di insiemi finiti o numerabili sono al più numerabili.*

Dimostrazione. Ricordiamo la possibilità di dimostrare il teorema ricorrendo allo schema di 'matrice infinita' (vedi la dimostrazione del teorema

1.2.5): dove è necessario AS? Anzitutto, si può supporre che gli a_m siano a due a due disgiunti, sostituendo ad a_1, $a_1 \setminus a_0$,..., ad a_n, $a_n \setminus (\cup_{j=0}^{n-1} a_j)$; non è poi restrittivo supporre tutti questi insiemi diversi dal vuoto. Se la famiglia di insiemi di cui fare adesso l'unione è finita, non c'è bisogno di AS, che è indispensabile se la famiglia è infinita. In quest'ultimo caso AS entra nella scelta delle biiezioni dei vari insiemi con qualche $k \in \omega$ o con ω, date per ipotesi, scelta necessaria per 'posizionare' gli elementi sulla varie righe. Più formalmente: data una simile unione $\cup_{m=0}^{\infty} a_m$, si sceglie per ogni m una biiezione $f_m : a_m \xrightarrow[\text{su}]{\text{1-1}} k_m \times \{m\}$ (o $f_m : a_m \xrightarrow[\text{su}]{\text{1-1}} \omega \times \{m\}$). Allora

$$\cup_{m=0}^{\infty} f_m : \cup_{m=0}^{\infty} a_m \xrightarrow{1-1} \omega \times \omega$$

e quindi l'unione è (al più) numerabile. $\square$

Teorema 3.2.21. ***(Hamel, 1905)*** *Ogni spazio vettoriale ha una base.*

Il teorema originale di Hamel concerne l'esistenza di una base per $\mathbb{R}$ come spazio vettoriale su $\mathbb{Q}$; anche per questo risultato è necessario AS (in sua assenza, uno spazio vettoriale può non avere basi, o averne di differente cardinalità). Hamel da questo risultato ricavò soluzioni discontinue dell'equazione funzionale $f(x + y) = f(x) + f(y)$, $x, y \in \mathbb{R}$: già Cauchy aveva provato che le funzioni reali continue soluzioni dell'equazione potevano essere soltanto $f(x) = kx$, $k \in \mathbb{R}$. Per dettagli, vedi sempre [Moore 1982, 2.5].

3.2.4 Conclusioni: l'indipendenza di AS da ZF

Nonostante lo scetticismo e le polemiche, i paradossi e le situazioni patologiche a cui talvolta AS dà luogo, la sua grande importanza per provare teoremi generali in matematica fa sì che ormai questo assioma sia considerato parte integrante della teoria degli insiemi: però, specie nella ricerche sui fondamenti, lo si menziona esplicitamente nelle dimostrazioni in cui risulta indispensabile: ZF con l'assioma di scelta viene indicato con ZFC ('C' per 'choice'). La sua accettazione dipese anche dalla dimostrazione di Gödel della consistenza di AS con ZF (o, che è lo stesso, con ZF^-):

Teorema 3.2.22. ***(Gödel, 1938)*** *Se ZF è consistente, lo è anche ZFC, giacché $ZF \nvdash \neg AS$: AS non è refutabile in ZF.*

Gödel ottenne questo risultato presentando una assiomatizzazione della teoria, equivalente a ZF, (vedi sezione 5.2) e un suo modello in cui AS è valido. Rimaneva il problema, più complesso, di provare l'*indipendenza* di AS da ZF, dimostrando la non derivabilità di ZF. Questo risultato fu ottenuto da P.J. Cohen:

Teorema 3.2.23. ***(Cohen, 1963)*** *AS non è derivabile in ZF: $ZF \nvdash AS$.*

Per prove di questi classici teoremi, si possono consultare [Kunen 1980] o [Smullyan-Fitting 1996].

Come nel caso di quella di Gödel, anche questa per questa prova è stato necessario elaborare metodi completamente nuovi e potenti in logica: l'assioma di scelta anche in questo modo ha contribuito notevolmente allo sviluppo della matematica del XX secolo.

3.3 L'ipotesi del continuo

Dopo la scoperta delle diverse potenze degli insiemi numerici, Cantor si pose il problema di studiare le connessioni tra l'infinito numerabile e la potenza del continuo: una relazione fu data dal teorema sulla potenza 1.2.17, ma una domanda si poneva naturalmente: vi erano insiemi con potenza intermedia? La ricerca poteva evidentemente farsi tra i sottoinsiemi di $\mathbb{R}$, ma nessun indizio fu trovato sull'esistenza o meno di insiemi del genere.

Cantor formulò allora l'ipotesi che non ve ne fossero:

Ipotesi del continuo [CH]
Ogni sottoinsieme infinito di $\mathbb{R}$ o è numerabile o ha la potenza del continuo

L''ipotesi' restò non dimostrata e perciò ha conservato questo nome; essa è del resto in contrasto con quanto accade nel caso finito: se un insieme ha n

elementi, il suo insieme potenza ne ha 2^n (da cui il nome) e quindi vi sono usualmente insiemi di potenza intermedia. In connessione con la sua teoria dei numeri cardinali e ordinali, Cantor tentò anche di provare una ipotesi più generale, sperando, come talvolta accade, che si dimostrasse più facile a provarsi:

Ipotesi generalizzata del continuo [GCH]
Non esistono potenze intermedie tra quella di un insieme infinito e quella del suo insieme delle parti

Cantor non riuscì mai a provare né l'una né l'altra, né a refutarle, ma ciò non era di fatto possibile. Ciò fu provato, a distanza di decenni, dai risultati di Gödel e Cohen:

Teorema 3.3.1. ***(Gödel, 1938)*** *Se ZF è consistente, $ZFC \cup \{GCH\}$ anche lo è: quindi $ZFC \nvdash \neg GCH$.*

Gödel ottenne questo risultato presentando un modello di ZF in cui anche GCH e AS sono validi. L'*indipendenza* di CH da ZFC fu ottenuta ancora una volta da P.J. Cohen, presentando un modello di ZFC in cui CH *non* vale:

Teorema 3.3.2. ***(Cohen, 1963)*** *Se ZF è consistente, da ZFC non si può derivare CH: cioè $ZFC \nvdash CH$. Equivalentemente, è consistente anche $ZFC \cup \{\neg CH\}$.*

A maggior ragione, in questo modello non vale GCH. Del resto si ha anche (vedi [Moore 1982, 5.1]):

Teorema 3.3.3. ***(Sierpiński, 1947)*** *In ZF, l'ipotesi generalizzata del continuo implica l'assioma di scelta:*

$$ZF \vdash GCH \Rightarrow AS.$$

In questo caso, l'ipotesi generalizzata del continuo è riferita a numeri cardinali e non a potenze di insiemi infiniti qualunque.
Per una ampia discussione di tutti questi ultimi teoremi, vedi l'approfondita trattazione in [Smullyan-Fitting 1996].

Capitolo 4

Numeri ordinali e cardinali

4.1 Cantor e il concetto di numero

Uno dei principali scopi di Cantor nel creare una teoria generale degli insiemi fu quello di ampliare la nozione di numero naturale nel suo duplice apetto, cardinale e ordinale, per mezzo di corrispondenze biunivoche (numeri cardinali), di insiemi bene ordinati e di similitudini (numeri ordinali) [1]. Egli intendeva introdurre enti come i 'numeri cardinali' o i 'numeri ordinali' per astrazione: per esempio, in un caso finito, il numero cardinale 'cinque' rappresenterebbe quanto in comune avessero gli insiemi in corrispondenza biunivoca con l'insieme di lettere $\{\alpha; \beta; \gamma; \delta; \epsilon\}$, senza considerare le caratteristiche degli elementi e il loro ordine nei vari insiemi; nel caso ordinale, si sarebbe dovuto considerare invece anche l'ordine con cui si presentavano. Lo stesso per analogia avrebbe dovuto accadere per i numeri cardinali e ordinali infiniti (di solito in questo contesto chiamati *transfiniti*).

L'introduzione –come insieme– della classe di tali insiemi quale possibilità per definire 'cinque' fu la strategia proposta da G. Frege per riassorbire l'aritmetica —e perciò l'intera matematica— nella logica; ma si è visto nel capitolo 1 come questo porti a contraddizione.

[1]Per le relative definizioni rinviamo a A.3.2.

4.1.1 Le cardinalità

In questa sottosezione presentiamo dunque una esposizione non troppo formalizzata della teoria dei numeri cardinali senza dare un significato autonomo a espressioni come 'la cardinalità (potenza) dell'insieme A', ma solo a espressioni come 'la cardinalità dell'insieme A è uguale (o maggiore, o minore) di quella dell'insieme B'; un po' come in geometria si può parlare di maggiore o minore lunghezza di un segmento rispetto a un altro, senza per questo introdurre una unità di misura.

Definizioni 4.1.1. (Vedi sempre A.3.2)

- $card(A) = card(B)$ (o anche $|A| = |B|$) significa semplicemente che $A \sim B$, cioè che esiste una corrispondenza biunivoca (o funzione biiettiva) da A su B: se interessa mettere in evidenza una tale corrispondenza f, si specifica $A \overset{f}{\sim} B$. Si dice pure che A e B sono *equipotenti*, o che hanno la stessa *potenza*.

- $card(A) \leq card(B)$ (o anche $|A| \leq |B|$) significa che esiste una funzione iniettiva da A in B, cioè che A è equipotente a un sottoinsieme di B.

- $card(A) < card(B)$ (o anche $|A| < |B|$) significa poi che esiste una funzione iniettiva da A in B, ma non accade che $A \sim B$: vi è una $f : A \xrightarrow{1-1} B$, ma nessuna tale f può essere *su* B. Dunque $card(A) =$ $= card(B)$ esclude $card(A) < card(B)$.

Osservazioni 4.1.2. • La relazione identica I_A su A è una corrispondenza biunivoca $I_A : A \xrightarrow[\text{su}]{\text{1-1}} A$, sicché $card(A) = card(A)$.

- Se $f : A \xrightarrow[\text{su}]{\text{1-1}} B$ e $g : B \xrightarrow[\text{su}]{\text{1-1}} C$ si ha subito

$$g \circ f : A \xrightarrow[\text{su}]{\text{1-1}} C \text{ e } f^{-1} : B \xrightarrow[\text{su}]{\text{1-1}} A.$$

Dunque se $A \overset{f}{\sim} B$ e $B \overset{g}{\sim} C$ si ha $A \overset{g \circ f}{\sim} C$ e anche $B \overset{f^{-1}}{\sim} A$. In altri termini, $card(A) = card(B)$ e $card(B) = card(C)$ implicano

$$card(B) = card(A) \text{ e } card(A) = card(C)$$

Se le precedenti sono proprietà ovvie che giustificano l'uso dei segni di disuguaglianza (e di uguaglianza), molte altre, in apparenza ugualmente elementari non sono altrettanto facilmente derivabili dalle definizioni: ad esempio, che valga una sorta di proprietà antisimmetrica per $\leq$ è una conseguenza di un teorema che Cantor diede per scontato, ma che fu provato solo in séguito. È il teorema 1.2, che qui riportiamo:

Teorema 4.1.3. *Se esistono* $f : A \xrightarrow{1-1} B$ *e* $g : B \xrightarrow{1-1} A$, *allora* $A \sim B$. *Dunque* $card(A) \leq card(B)$ *e* $card(B) \leq card(A)$ *implicano* $card(A) =$
$= card(B)$.

Corollario 4.1.4. *(a) Da* $card(A) < card(B)$ *e* $card(B) < card(C)$ *segue* $card(A) < card(C)$, *e lo stesso vale se una delle due disuguaglianze nell'ipotesi è un* $\leq$.

(b) Delle tre possibilità $card(A) < card(B)$, $card(A) = card(B)$, $card(B) <$
$< card(A)$, *ne vale al più una.*

Dimostrazione. (a) Risulta comunque $card(A) \leq card(C)$; supponiamo $card(A) \leq card(B)$ e sia $f : A \xrightarrow{1-1} B$, eventualmente *su* B. Per assurdo, sia $g : C \xrightarrow[\text{su}]{\text{1-1}} A$; allora $f \circ g : C \xrightarrow{1-1} B$, che per il teorema precedente va contro l'ipotesi $card(B) < card(C)$. Dimostrazione analoga per $card(B) \leq card(C)$. (b) Basta provare che $card(A) < card(B)$ e $card(B) < card(A)$ si escludono a vicenda: ma questo è immediato dalla parte (a) della dimostrazione e da $card(A) = card(A)$. $\square$

In base a quanto si è già visto (in particolare, nel corollario 3.2.13), se $m, n \in \omega$ e $m < n$ si ha poi

Proposizione 4.1.5.

- $card(m) < card(n)$, $card(n) < card(\omega)$,
- $card(\omega) < card(\mathcal{P}(\omega))$ *e in generale, se* A *è un insieme qualunque,* $card(A) < card(\mathcal{P}(A))$.

Per quanto vedremo in séguito, conviene porre $j = card(j)$ se $j \in \omega$ oppure $j = \omega$: i numeri naturali sono qui gli elementi di ω.

Per avere un buon parallelo con le consuete disuguaglianze, due insiemi A e B dovrebbero però essere sempre comparabili per cardinalità:

- **(Legge di dicotomia)** Vale sempre almeno una delle due possibilità: $card(A) \leq card(B)$ oppure $card(B) \leq card(A)$.
- **(Legge di tricotomia)** Vale sempre una e una sola delle tre possibilità: $card(A) < card(B)$ *aut* $card(A) = card(B)$ *aut* $card(B) < card(A)$.

Le due leggi sono equivalenti, ma come si vedrà, è indispensabile l'assioma di scelta per provarle: è questo uno dei risultati più importanti legati ad AS.

4.1.2 I tipi d'ordine

Esaminiamo ora, in analogia con le proprietà legate alle biiezioni, quelle connesse alle similitudini (vedi A.3.2). Se due buoni ordinamenti sono simili si dice che hanno lo stesso *tipo d'ordine*; il tipo, definibile anche per ordinamenti più generali, nel caso dei buoni ordinamenti ha proprietà analoghe, anzi migliori, della cardinalità.

Definizioni 4.1.6.

- Se $(A; <_A) \approx (B; <_B)$ i due ordinamenti hanno tipi uguali: $tipo(A; <_A) = tipo(B; <_B)$, o semplicemente, lasciando sottointese le relazioni, $tipo(A) = tipo(B)$.
- Se $(A; <_A)$ è simile a un segmento iniziale $seg(z) = seg(z; B; <_B)$ di B, si dice che il tipo di A è minore di quello di B: $tipo(A; <_A) < tipo(B; <_B)$ o più semplicemente $tipo(A) < tipo(B)$.
- Infine, $tipo(A) \leq tipo(B)$ significa $(tipo(A) < tipo(B) \vee tipo(A) = = tipo(B))$.

Siano ora A, B, C bene ordinati da $<_A$, $<_B$ e $<_C$ rispettivamente.

Osservazioni 4.1.7.

- Se $A \overset{f}{\approx} B$ e $B \overset{g}{\approx} C$, allora $A \overset{g \circ f}{\approx} C$: quindi $tipo(A) = tipo(B)$ e $tipo(B) = tipo(C)$ implicano $tipo(A) = tipo(C)$; poiché allora $B \overset{f^{-1}}{\approx} A$, da $tipo(A) = tipo(B)$ segue $tipo(B) = tipo(A)$.

Infine, dato che l'identità I_A è anche ovviamente una similitudine, si ha sempre $tipo(A) = tipo(A)$.

- Analogamente si verifica che $tipo(A) < tipo(B)$ e $tipo(B) < tipo(C)$ implicano $tipo(A) < tipo(C)$.

Esercizi 4.1.8. In 4.2 si vedrà che ω e i numeri naturali sono bene ordinati dalla relazione di appartenenza $\in$ (ristretta ai loro elementi) e, se $m < n$, si ha $tipo(m) < tipo(n)$ e $tipo(m) < tipo(\omega)$. In questi casi si omette di specificare 'tipo': $tipo(m) = m$, eccetera.

Se si riesaminano le proprietà dei tipi, ci si accorge che è meno scontato provare ad esempio che $(A; <_A)$ non è mai simile a un suo segmento iniziale. Questo tuttavia segue da risultati fondamentali che fanno dei buoni ordinamenti relazioni veramente 'buone'. Cominciamo con un utile lemma.

Lemma 4.1.9. *Se A è bene ordinato da $<_A$ e $B \subseteq A$, esso è bene ordinato sempre da $<_A$: allora ogni similitudine $A \overset{f}{\approx} B$ è tale che $a \leq_A f(a)$ per ogni $a \in A$.*

Dimostrazione. Scriviamo semplicemente $<$ anziché $<_A$. Per assurdo, sia $f(b) < b$ per un $b \in A$: allora si può supporre che b sia il *minimo* elemento con tale proprietà, per la definizione stessa di buon ordine. Ma, essendo $f(b) = c < b$, risulterà $f(b) = c \leq f(c) = f(f(b))$, mentre f è una similitudine e quindi dovrebbe essere $f(f(b)) < f(b)$. □

Da questo lemma seguono conclusioni importanti:

Proposizione 4.1.10. *Se $(A; <_A) \overset{f}{\approx} (B; <_B)$, la similitudine f è unica.*

Dimostrazione. Se vi sono due similitudini $A \overset{f}{\approx} B$ e $A \overset{g}{\approx} B$, allora $A \overset{f^{-1}\circ g}{\approx} A$ e quindi per ogni $a \in A$, $a \leq f^{-1} \circ g(a)$, cioè $f(a) \leq g(a)$. Scambiando f con g si ottiene $g(a) \leq f(a)$ e quindi $f = g$. □

Proposizione 4.1.11. *Nessun insieme bene ordinato è simile a un suo segmento iniziale. Quindi è impossibile che sia $tipo(A) < tipo(A)$.*

Dimostrazione. Indichiamo al solito la relazione con $<$. Per assurdo, se fosse $A \overset{f}{\approx} seg(x; A)$, si avrebbe, per ogni $y \in A$, $f(y) \in seg(x; A)$ e quindi $f(y) < x$. In particolare, $f(x) < x$, contro il lemma. $\square$

Teorema 4.1.12. *Vale la legge di tricotomia per i tipi di buon ordine, cioè per ogni coppia di buoni ordinamenti* $(A; <_A)$, $(B; <_B)$ *o essi sono simili, o uno è simile a un segmento iniziale dell'altro, e vale esattamente una ed una soltanto di queste tre possibilità. Quindi*

$$tipo(A; <_A) < tipo(B; <_B) \text{ aut } tipo(A; <_A) = tipo(B; <_B) \text{ aut }$$
$$tipo(B; <_B) < tipo(A; <_A).$$

Dimostrazione. (Traccia) Non specifichiamo le diverse relazioni d'ordine. Consideriamo il sottoinsieme A_0 di A degli $x \in A$ per cui esiste $y \in B$ tale che $seg(x; A) \approx seg(y; B)$. y è determinato univocamente da x e perciò possiamo porre $y = f(x)$: $A_0 = dom(f)$. Sia $B_0 = Im(f)$: A_0 coincide con tutto A oppure ne è un segmento iniziale; lo stesso per B_0 rispetto a B; f è una similitudine tra essi. Non può essere $A_0 \subset A$ e contemporaneamente $B_0 \subset B$: basterebbe considerare il minimo $x \notin A_0$ e fargli corrispondere il minimo $y \notin B_0$ per prolungare f. Gli altri tre casi possibili si escludono a vicenda e danno la legge di tricotomia. $\square$
Per una diversa dimostrazione, vedi [Halmos 1980, cap.18].

Dunque, a differenza delle cardinalità, i tipi di (buon) ordine sono sempre confrontabili: da questo dipende l'importanza del teorema del buon ordinamento di Zermelo 3.2.2, e quindi dell'assioma di scelta: se ogni insieme è bene ordinabile, tramite una similitudine, che è una funzione iniettiva, si può sempre determinare se $card(A) \leq card(B)$ oppure se $card(B) \leq card(A)$. Vale quindi la legge di dicotomia (e quella di tricotomia ne segue) per le cardinalità.

Rimane comunque il problema di trovare posto nella teoria degli insiemi a questi 'numeri'. Esso fu brillantemente risolto da von Neumann con una strategia tradizionale: si introducono 'unità di misura' per la cardinalità e l'ordinalità per mezzo di particolari insiemi, la cui esistenza si può provare in ZF e si paragonano (usando AS) con questi gli altri insiemi mediante corrispondenze biunivoche o similitudini. Come le seconde sono casi particolari delle prime, i numeri cardinali sono particolari numeri ordinali; i numeri naturali sono al tempo stesso cardinali e ordinali. È possibile anche vedere in questa teoria uno sviluppo dei "princìpi di generazione dei numeri" enunciati da Cantor stesso [Dauben 1979, pagg.97-98 e 205-206]:

1. passare da un numero al successivo per "ripetute addizioni di unità"

2. "formare il limite di quanto già ottenuto contando [e procedere oltre]"

che sono in definitiva i due aspetti, ordinale (1) e cardinale (2) del numero, anche se Cantor li enunciò specificamente a proposito degli ordinali, che godevano di un ruolo privilegiato al proposito. Del resto, questa distinzione si ripropone anche tra i numeri dello stesso tipo, come si vedrà.

4.2 I numeri ordinali

Il fatto che i numeri naturali siano bene ordinati da $\in$, così come ω, non è fortuito, ma un caso particolare di una definizione che permette di introdurre e studiare come insiemi *numeri ordinali* —i numeri naturali, ma anche ordinali infiniti (*transfiniti*), senza passare dall'espressione, di per sé priva di significato insiemistico, di 'tipo', non usabile correttamente senza qualche relazione di uguaglianza o disuguaglianza. Come caso particolare dei numeri ordinali, sarà possibile introdurre anche i *numeri cardinali*, senza riferimento alla 'cardinalità'. Assumiamo ZFC (ma vi sarà bisogno di AS solo in casi particolari) e cominciamo con la definizione di (numero) ordinale. Nel séguito ometteremo diverse dimostrazioni: per esse, il rinvio è a [Kunen 1980, cap.1, §7] o a [Abian 1972, Capp.VII e VIII].

Definizioni 4.2.1. 1. Un insieme a si dice transitivo se ogni suo elemento x ne è anche un sottoinsieme: $\forall x \in a\ (x \subseteq a)$. Equivalentemente, $\forall x \forall y (y \in x \in a \Longrightarrow y \in a)$, il che giustifica la terminologia.

2. Un insieme a che sia transitivo e bene ordinato da $\in$ o, più esattamente, da $\in_a$, dove
$$x \in_a y \Longleftrightarrow x \in a \wedge y \in a \wedge x \in y$$
si chiama un numero ordinale (di von Neumann) o, brevemente, un ordinale.

Osservazioni 4.2.2.
- Un ordinale si indica di solito con lettere minuscole dell'alfabeto greco: $\alpha, \beta, \gamma, \ldots$ e le relative quantificazioni si intendono limitate relativamente alla proprietà di essere un ordinale, $\mathbf{ORD}(v)$, che formalizza la definizione precedente. Ad esempio $\forall \alpha \ldots$ sta per $\forall v\,(\mathbf{ORD}(v) \Longrightarrow \ldots)$. Coerentemente con le osservazioni 2.0.4, **ORD** può essere interpretata come una classe e si vedrà che si tratta di una classe propria: il grassetto maiuscolo indica ancora proprietà (predicati) interpretati estensionalmente come classi.

- Non troppo sistematicamente, e senza alcun valore teorico, si indicano poi elementi generici con lettere latine minuscole (ma $m, n, \ldots$ indicano al solito numeri naturali), i relativi insiemi con lettere latine maiuscole, le famiglie di insiemi con lettere calligrafiche maiuscole (come $\mathcal{F}, \mathcal{G}, \ldots$) per semplicità di lettura: si tratta pur sempre di insiemi.

- La relazione $\in$ in quanto buon ordinamento di un ordinale α si indica anche con $<$ ($\in_\alpha$, $<_\alpha$ se necessario specificare).

- Come già osservato, i numeri naturali zero compreso, sono ordinali.

- Si noti che per transitività, se α è un ordinale,
$$\ldots u \in v \in w \in x \in y \in \alpha \text{ implica } u, v, w, x \in \alpha$$
il buon ordinamento dato da $\in$ assicura che queste catene sono sempre finite, e quindi $\emptyset = 0$ è sempre elemento di qualsiasi ordinale non vuoto. Un ordinale è sempre un insieme ben fondato (e regolare) a prescindere dall'assioma di fondazione o di regolarità.

- Si noti la differenza essenziale tra la transitività della relazione binaria $\in_\alpha$ e la transitività di α stesso, che la infelice terminologia porta a confondere: un insieme A può essere transitivo e non essere bene ordinato da $\in_A$ (esempio: $A = \{0; 1; \{1\}\}$) oppure al contrario essere bene ordinato da $\in_A$ e non essere transitivo (esempio: $A = \{0; 3; 5\}$). Provarlo per esercizio: naturalmente 0, 1 eccetera sono numerali di von Neumann.

Teorema 4.2.3. *α, β, γ siano ordinali.*

1. *Se $x \in \alpha$, allora x è anch'esso un ordinale, e $x = seg(x; \alpha; \in_\alpha)$. Quindi, se β, $\gamma \in \alpha$, $seg(\beta; \alpha; \in_\alpha) \subset seg(\gamma; \alpha; \in_\alpha)$ se e solo se $\beta \in \gamma$.*

2. *Se $\alpha \in \beta$ e $\beta \in \gamma$, allora $\alpha \in \gamma$.*

3. *$\alpha \notin \alpha$.*

4. *Se $\alpha \approx \beta$, allora $\alpha = \beta$.*

5. *(Legge di tricotomia per gli ordinali) Aut $\alpha \in \beta$ aut $\alpha = \beta$ aut $\beta \in \alpha$.*

6. *Se $\mathbf{C}$ è una classe non vuota di ordinali, essa ha un (unico) $\in$-minimo, cioè esiste $\alpha \in \mathbf{C}$ tale che $\alpha \in \mathbf{C} \wedge \forall \beta \in \mathbf{C}(\alpha \in \beta \vee \alpha = \beta)$. α viene indicato con $\min \mathbf{C}$ e coincide con $\bigcap \mathbf{C}$.*

7. *Il successore insiemistico di α, $S(\alpha) = \alpha \cup \{\alpha\}$ è anch'esso un ordinale, diverso da α, e il minimo maggiore di esso: $S(\alpha)$ si dice* ordinale successore. *Inoltre, $S(\alpha) = S(\beta)$ implica $\alpha = \beta$.*

Dimostrazione.

1. Se $x \in \alpha$ allora $x \subseteq \alpha$ e perciò x è bene ordinato da $\in_\alpha$; se poi $z \in y \in x$ si ha che anche $z, y \in \alpha$ e per transitività di $\in_\alpha$, $z \in x$: dunque $y \subseteq x$ e x risulta transitivo. Le ultime affermazioni sono immediate.

2. Segue immediatamente dalla transitività di γ.

3. È immediato, per assurdo, dal fatto che $\in_\alpha$ è una relazione irriflessiva come conseguenza della definizione.

4. Sia $\alpha \overset{f}{\approx} \beta$: proviamo che $f(x) = x$ per ogni $x \in \alpha$. Per assurdo, esista un $x \in \alpha$ tale che $x \neq f(x)$: si può supporre che sia l'elemento $\in_\alpha$-minimo con tale proprietà. Ma allora sarebbe, per 1, (vedi anche A.3.2)

$$x = seg(x; \alpha; \in_\alpha) = f[seg(x; \alpha; \in_\alpha)] = seg(f(x); \beta; \in_\beta) = f(x)$$

(perché per gli $y \in seg(x; \alpha; \in_\alpha)$ risulta $f(y) = y$) e quindi $x = f(x)$, da cui l'assurdo.

5. Si usino il teorema 4.1.12 e i risultati precedenti.

6. Si fissi un $\alpha_0 \in \mathbf{C}$: se esso è il minimo cercato, non c'è nulla da provare; altrimenti, per la legge di tricotomia, esisteranno $\beta \in \mathbf{C} \cap \alpha_0$ [2] : si prenda il minimo di questi β, che è anche il minimo cercato. Indichiamolo con $\alpha = min\,\mathbf{C}$, e sia $\gamma \in \mathbf{C}$: allora $\alpha \subseteq \gamma$ e quindi $\alpha \subseteq \bigcap_{\gamma \in \mathbf{C}} \gamma = \bigcap \mathbf{C}$; d'altra parte $\alpha \in \mathbf{C}$ e quindi $\bigcap \mathbf{C} \subseteq \alpha$, da cui l'uguaglianza.

7. Che $\alpha \subset S(\alpha)$ segue immediatamente da 3. Tutti gli elementi di $S(\alpha)$ sono ordinali: da questo e dalla sua definizione segue subito che esso è transitivo e bene ordinato da $\in_{S(\alpha)}$. Non vi sono ovviamente ordinali γ tali che $\alpha < \gamma < S(\alpha)$. Infine, l'ultima affermazione segue facilmente dalla legge di tricotomia, dato che $\alpha \in S(\beta)$ implica $\alpha \in \beta \vee \alpha = \beta$ e $\beta \in S(\alpha)$ implica $\beta \in \alpha \vee \beta = \alpha$. $\square$

Ecco due utili corollari del teorema.

Corollario 4.2.4. *Un insieme transitivo A di ordinali è un ordinale.*

Dimostrazione. Siano $\alpha \in_A \beta \in_A \gamma$ elementi di A: allora $\alpha \in_A \gamma$; le altre proprietà di $\in_A$ derivano dal teorema 4.2.3. $\square$

[2] $\mathbf{C} \cap \alpha_0 = \{x \in \alpha_0;\ \mathbf{C}(x)\}$ è ben definito per specificazione.

Corollario 4.2.5. *α, β siano ordinali. $\alpha \subset \beta$ se e solo se $\alpha \in \beta$. $\alpha \subseteq \beta$ se e solo se $\alpha \in \beta$ aut $\alpha = \beta$.*

Dimostrazione. Immediata, dalla legge di tricotomia, n.5. □

D'ora in poi indicheremo spesso, come già detto, $\in$ con $<$.

Osservazione 4.2.6. Il n.7 del teorema può essere generalizzato in: *il successivo di un insieme ben fondato x è ben fondato e diverso da x.* Se però, in assenza di AF, fosse $x = \{x\}$, si avrebbe $x = S(x)$.

Per alcune parti del teorema precedente, si vede che se **ORD** fosse un insieme, sarebbe per definizione un ordinale: ma questo contraddice il n.7 dello stesso teorema, giacché dovrebbe essere $\mathbf{ORD} \in S(\mathbf{ORD}) \in \mathbf{ORD}$, assurdo. Si ottiene allora il primo pubblicato (1897: vedi [Dauben 1979, pagg.259-60]) tra i tre paradossi più famosi riguardanti la teoria cantoriana degli insiemi:

Paradosso di Burali-Forti
Non esiste un insieme che abbia per elementi tutti gli ordinali

In altri termini, **ORD** è una classe propria, cioè può essere trattata in ZFC soltanto come una proprietà $\mathbf{ORD}(x)$.

Abbiamo introdotto in 2.4 i numeri naturali indirettamente, come elementi di ω, il più piccolo insieme induttivo (definizione 2.4.2), ma finora ne abbiamo usato le proprietà elementari giustificandole sulla base dell'intuizione; sebbene sia possibile ricavarle da quella definizione, è più agevole dare di essi una definizione diretta, che giustifica facilmente quanto visto finora al proposito. Si può infatti definire esplicitamente numeri naturali come particolari ordinali, riottenendo ω:

Definizione 4.2.7. L'ordinale α è un numero naturale se è $\alpha = \emptyset$ oppure se è un successore e i suoi elementi sono tutti $\emptyset$ oppure successori. Abbreviamo provvisoriamente questa proprietà di α con $N(\alpha)$.

Come sempre, indicheremo con 0 l'insieme vuoto, e in generale i numeri naturali con $j, m, \ldots$. Proviamo ora che ω coincide con l'insieme di questi ordinali.

Proposizione 4.2.8. *ω, il più piccolo insieme induttivo, ha per elementi esattamente i numeri naturali, cioè gli ordinali m per cui vale $N(m)$.*

Dimostrazione.

1. Proviamo anzitutto che $N(m)$ *implica* $N(S(m))$. Se $m = 0$, ciò è immediato, dato che $S(0) = \{0\}$. Supponiamo che $N(m)$ valga per un $m \neq 0$: allora m è un successore, e i suoi elementi sono 0 o successori. Ora $S(m) = m \cup \{m\}$: i suoi elementi sono quelli di m, più m stesso: sono tutti 0 o successori, quindi $N(S(m))$.

2. Viceversa, *se m è un successore e un numero naturale, $m = S(j)$ e j è un naturale*: infatti, $j \in m$ e quindi è 0 o un successore; se $j \neq 0$ i suoi elementi sono elementi di m (per la transitività di m stesso) e quindi 0 o successori.

3. Sia ora c un insieme induttivo. Proviamo che $N(m)$ *implica* $m \in c$. Ciò è immediato se $m = 0$; sia allora per assurdo $m \neq 0$ tale che $m \notin c$: si può supporre che m sia il minimo naturale con queste proprietà . Ma allora $m = S(j)$ è il successore di un numero naturale $j < m$ per 2 e si avrebbe (per minimalità di m) $j \in c$ da cui, per induttività di c, $m \in c$, contraddizione.

4. Come conseguenza di 3, ogni numero naturale è elemento di ω e pertanto i numeri naturali costituiscono un insieme, che è induttivo per 1 e dunque il loro insieme coincide con ω per minimalità di ω stesso. $\square$

A questo punto, si può verificare che ω soddisfa gli assiomi di Peano [3] : i primi quattro derivano da questi risultati sui numeri naturali intesi come ordinali, mentre il principio di induzione segue dalla definizione di ω come il

[3] Vedi *Appunti sulla ricorsività*, 4.1.

minimo insieme induttivo.
Si può inoltre verificare direttamente che ω è un ordinale (corollario 4.2.4), ma questo segue anche dalla proposizione seguente, dato che $\omega = \cup_{m\in\omega} m$ (esercizio).

Proposizione 4.2.9. *Se $\mathcal{F}$ è una famiglia di ordinali, $\bigcup \mathcal{F} = \bigcup_{\beta\in\mathcal{F}} \beta$ è un ordinale.*

Dimostrazione. Tralasciamo i casi banali di $\mathcal{F} = \emptyset$ o $\mathcal{F} = \{\emptyset\}$. Sia $\gamma \in \bigcup \mathcal{F}$: allora esiste un $\beta \in \mathcal{F}$ tale che $\gamma \in \beta$: quindi $\gamma \subset \beta \subseteq \bigcup \mathcal{F}$ e quindi $\bigcup \mathcal{F}$ è transitivo. Il corollario 4.2.4 garantisce allora la conclusione. □

Corollario 4.2.10. *$\bigcup \mathcal{F}$ è il minimo ordinale $\geq$ di tutti gli elementi di $\mathcal{F}$: viene indicato anche con $\sup \mathcal{F}$.*

Corollario 4.2.11. *α è un ordinale successore se e solo se $\bigcup \alpha \subset \alpha$. In tal caso, se $\beta = \bigcup \alpha$, risulta $\alpha = S(\beta)$. In caso contrario, $\alpha = \bigcup \alpha$.*

Dimostrazione. In ogni caso, per transitività di α, $\bigcup \alpha \subseteq \alpha$.
($\Rightarrow$) Sia $\alpha = S(\beta)$: allora $\beta \in \alpha$, ma $\beta \notin \bigcup S(\beta)$, da cui la tesi.
($\Leftarrow$) Applichiamo più volte il corollario 4.2.5. Sia $\beta = \bigcup \alpha \subset \alpha$: allora $\beta \in \alpha$. Quindi $S(\beta) = \beta \cup \{\beta\} \subseteq \alpha$. Se fosse $S(\beta) \subset \alpha$ si avrebbe $\beta \in S(\beta) \in \alpha$, da cui $\beta \in \bigcup \alpha = \beta$, un assurdo; quindi deve essere $S(\beta) = \alpha$. □
Il corollario precedente permette una partizione degli ordinali in tre classi disgiunte (o, più esattamente, in due classi, più l'insieme vuoto):

Definizione 4.2.12. Ogni ordinale α è:

- l'ordinale zero: $\alpha = \emptyset = 0$, oppure
- un ordinale successore: $\exists \beta\, (\alpha = S(\beta))$, oppure
- un ordinale *limite*, per cui $\alpha = \bigcup_{\beta<\alpha} \beta$.

Gli ordinali successori e limite corrispondono alle due cantoriane leggi di generazione dei numeri. I numeri naturali diversi da 0 sono ordinali successori, mentre ω è un ordinale limite (il minimo tra questi: perché?); questo in base alla definizione, ma può provarlo anche la seguente osservazione generale:

Proposizione 4.2.13. *L'estremo superiore β di una famiglia $\mathcal{F}$ non vuota di ordinali, se non è un massimo, è necessariamente un ordinale limite.*

Dimostrazione. Certamente, se $\beta = sup\,\mathcal{F} \notin \mathcal{F}$, risulta $\beta \neq 0$. Dobbiamo provare che $\beta = \bigcup_{\alpha\in\beta}\alpha$: per quanto osservato nella dimostrazione del corollario appena visto (4.2.11), basta dimostrare che $\beta \subseteq \bigcup_{\alpha\in\beta}\alpha$. Dato $\gamma \in \beta = \bigcup_{\alpha\in\mathcal{F}}\alpha$, proviamo dunque $\gamma \in \bigcup_{\alpha\in\beta}\alpha$. Risulta $\gamma \in \alpha$ per qualche $\alpha \in \mathcal{F}$; $\alpha \subseteq \beta$ e, per tricotomia, $\alpha = \beta$ aut $\alpha \in \beta$. La prima alternativa è esclusa ($\beta \notin \mathcal{F}$) e quindi $\gamma \in \alpha \in \beta$, da cui $\gamma \in \bigcup_{\alpha\in\beta}\alpha$, come si doveva dimostrare. □

Gli ordinali generalizzano, dei numeri naturali, le proprietà di induzione (chiamata adesso induzione *transfinita*): questo riguarda sia degli *schemi di dimostrazione* che il principio di induzione vero e proprio, riguardante la *definizione* di costruzioni insiemistiche dipendenti da un ordinale. Iniziamo dal primo caso.

Dimostrazione per induzione transfinita-1 Si debba provare che una proprietà $\phi = \phi(\alpha)$ vale per tutti gli ordinali α (possono comparire altre variabili, da intendere come parametri). Basta allora provare che

Per ogni α, se $\phi(\beta)$ vale per ogni $\beta < \alpha$, segue che vale $\phi(\alpha)$

Supponiamo di aver provato questo: basta allora ragionare per assurdo e supporre che vi sia un γ per cui *non* vale $\phi(\gamma)$. Si può anche supporre che γ sia il *minimo* ordinale per cui non vale ϕ (principio del minimo ordinale). Si ha subito un assurdo, dato che allora ϕ dovrebbe valere per ogni $\beta < \gamma$ e abbiamo provato che questo comporta appunto $\phi(\gamma)$.

Dimostrazione per induzione transfinita-2 Specializzando il ragionamento di sopra, supponiamo di aver provato che

- $\phi(0)$ vale;
- se per un β qualsiasi, vale $\phi(\beta)$, allora vale $\phi(S(\beta))$;

- Se α è un ordinale limite e $\phi(\beta)$ vale per ogni $\beta < \alpha$, allora vale anche $\phi(\alpha)$.

La dimostrazione è ancora per assurdo, ma suddivisa in tre casi, a seconda che il minimo γ per cui $\phi(\gamma)$ non vale sia: i) $\gamma = 0$, oppure ii) γ un successore, oppure iii) γ limite.

Dimostrazione per induzione transfinita-3 Si possono restringere le induzioni dei tipi 1 e 2 a provare che $\phi(\alpha)$ vale per ogni $\alpha < \delta$: basta considerare soltanto gli ordinali $< \delta$.

Il secondo caso, delle 'definizioni' per induzione, richiede costruzioni funzionali $\mathbf{F}$ definite su tutti gli insiemi —come $\mathcal{P}$, che associa univocamente a un insieme un altro insieme, il suo insieme delle parti. Sebbene le si possano indicare con $\mathbf{F} : \mathbf{U} \to \mathbf{U}$ o con $y = \mathbf{F}(x)$, questi modi di scrivere vanno intesi come un aiuto all'intuizione: si tratta di *fbf* $\phi(x; y)$ [4] tali che (in *ZF*) $\forall x \exists ! y \phi(x; y)$. Naturalmente lo stesso vale per costruzioni definite su altre classi proprie, come **ORD**. Si può allora enunciare il principio di induzione transfinita per definire costruzioni $\mathbf{G} : \mathbf{ORD} \to \mathbf{U}$ usando costruzioni $\mathbf{F} : \mathbf{U} \to \mathbf{U}$.

Teorema 4.2.14. *(Principio di induzione transfinita) Esiste una unica costruzione* $\mathbf{G} : \mathbf{ORD} \to \mathbf{U}$ *tale che, per ogni ordinale* α

$$\mathbf{G}(\alpha) = \mathbf{F}(\mathbf{G} \restriction \alpha) \tag{4.1}$$

Per una dimostrazione, vedi [Kunen 1980, cap.1, §9].

Osservazioni 4.2.15.

- La formula esprime l'idea che l'insieme $\mathbf{G}(\alpha)$ è determinato in maniera univoca dai valori di $\mathbf{G}$ sugli elementi di α, cioè sugli ordinali $\delta < \alpha$.
- Si capisce da questo come sia possibile, limitando la 4.1 agli α elementi di un ordinale specifico γ, ottenere una *funzione* G di dominio γ per

[4] Eventualmente possono anche qui comparire altre variabili libere, da intendere come parametri.

rimpiazzamento. In tal caso si parla di γ-*successione*, o successione di tipo γ. Le ω-successioni sono le successioni ordinarie, e in tal caso la definizione precedente è l'ordinaria *definizione per ricorsione* (su tutti i valori precedenti); le n-successioni ($n \in \omega$, $n \neq 0$) sono le *sequenze (di lunghezza n).*

- Un'altra variante (un caso particolare) si presenta quando $\mathbf{F}$ abbia una definizione per casi, a seconda che il suo argomento sia 0, o una funzione definita su un ordinale successore o limite, o altro, come nell'esempio successivo: le successioni ordinarie definite per ricorsione semplice (da n a $n+1$) rientrano in questo caso. Per una definizione dettagliata di $\mathbf{F}$ in casi del genere vedi pagina 86.

Descriviamo brevemente una importante applicazione del principio di induzione transfinita. Dato un ordinale α, definiamo per casi insiemi R_α con questo tipo di induzione [Kunen 1980, cap. III, §§2 e 4]:

$$\begin{cases} R_\alpha = 0 & \text{se} \quad \alpha = 0 \\ R_\alpha = \mathcal{P}(R_\beta) & \text{se} \quad \alpha = S(\beta) \text{ è un ordinale successore} \\ R_\alpha = \bigcup_{\gamma<\alpha}(R_\gamma) & \text{se} \quad \alpha \text{ è un ordinale limite.} \end{cases}$$

Se si pone $\mathbf{WF} = \bigcup_{\mathbf{ORD}(\alpha)} R_\alpha$, con ovvio significato per l'unione (pagina 39), si ha certamente una classe propria, dato che, sempre per induzione, $\alpha \in R_{S(\alpha)}$ per ogni α e quindi $\mathbf{ORD} \subset \mathbf{WF}$; d'altra parte con ZF^- (ZF senza l'assioma di regolarità) si può provare che in $\mathbf{WF}$ valgono gli assiomi di ZF^- più *Reg* (vedi 3.1). Dunque ogni modello di ZF^- contiene un sottomodello in cui vale anche quest'ultimo assioma e gli insiemi nei modelli in cui esso vale si possono descrivere in maniera gerarchica (si parla infatti di *gerarchia cumulativa degli insiemi*), come risultanti dalla iterazione transfinita della operazione di costruzione dell'insieme delle parti e di unione dei nuovi insiemi ottenuti: di qui la sua importanza nella teoria assiomatica. D'altra parte per inquadrare la matematica questo assioma non è di particolare rilevanza, perché può essere sempre presupposto e quindi non permette di ritrovare risultati essenzialmente nuovi.

Per sviluppare fin qui la teoria degli ordinali non occorre AS, e non occorre nemmeno se si vuole assegnare un tipo ad ogni insieme bene ordinato.

Teorema 4.2.16. *Ogni insieme bene ordinato* $(A; <_A)$ *è simile ad esattamente un ordinale* α*, il suo tipo: tipo*$(A; <_A) = \alpha$*.*

Dimostrazione. Mentre l'unicità del tipo è immediata dalla proposizione 4.1.10, non lo è l'esistenza, nonostante la legge di tricotomia: vedi [Kunen 1980, cap.1, §7.6]. □
AS (come teorema del buon ordinamento) occorre invece se si vuole attribuire un qualche tipo a ogni insieme: nel caso infinito però questo tipo non è certo unico. Bene ordinando ω in maniera non naturale si possono ottenere infiniti tipi d'ordine (ad esempio, con $1 < 2 < 3 < \ldots < 0$ si ha il tipo $S(\omega)$), mentre in qualunque modo venga bene ordinato n si ottiene sempre come tipo n stesso (perché?).

4.2.1 L'aritmetica ordinale

Sulla base della classificazione degli ordinali in 0, successori e limiti si possono definire le 'operazioni' fondamentali dell'*aritmetica ordinale*: addizione, moltiplicazione, elevamento a potenza. Ne accenniamo senza sviluppare in dettaglio l'algebra di queste 'operazioni'. Sviluppi e precisazioni si possono trovare, in [Abian 1972, loc. cit.] e [Kunen 1980, loc. cit.].

La definizione più naturale per la somma $\alpha + \beta$ di ordinali è senz'altro

contare α *e di séguito* β

Questo può essere realizzato con l'insieme $A = (\{0\} \times \alpha) \cup (\{1\} \times \beta)$ bene ordinato (con $<_A$) facendo precedere le coppie $(0; \gamma)$, $\gamma < \alpha$, ordinate con $\in_\alpha$ a tutte le coppie $(1; \delta)$, $\delta < \beta$, ordinate con $\in_\beta$. Si può porre allora

Definizione 4.2.17 (Addizione ordinale)**.**

$$\alpha + \beta = tipo(A; <_A)$$

Osservazione 4.2.18. A è la cosiddetta *unione disgiunta* di α e β: si tratta di un artificio per 'non sovrapporre' elementi comuni ai due insiemi, artificio facilmente estendibile al caso di una famiglia qualunque di insiemi. In questo caso, bisogna tenere distinti gli elementi comuni per dare una definizine ragionevole di somma; se fosse $\alpha < \beta$ si avrebbe altrimenti $\alpha \cup \beta = \beta \ldots$

Direttamente da questa definizione si ottengono le caratteristiche fondamentali dell'addizione:

Teorema 4.2.19. *(Proprietà fondamentali dell'addizione ordinale) Se α, β, γ sono ordinali*

1. $(\alpha + \beta) + \gamma = \alpha + (\beta + \gamma)$
2. $\alpha + 0 = 0 + \alpha = \alpha$ *e* $\alpha + 1 = S(\alpha)$
3. *Formule ricorsive per l'addizione:*

$$\alpha + \beta = \begin{cases} \alpha & \textit{se} \quad \beta = 0 \\ S(\alpha + \gamma) & \textit{se} \quad \beta \textit{ è un ordinale successore, } \beta = S(\gamma) \\ \bigcup_{\gamma<\beta}(\alpha + \gamma) & \textit{se} \quad \beta \textit{ è un ordinale limite, } \beta = \bigcup_{\gamma<\beta} \gamma \end{cases}$$

o, in termini più espliciti,

$$\begin{array}{lcl} \alpha + 0 & = & \alpha \\ \alpha + (\gamma + 1) & = & (\alpha + \gamma) + 1 \\ \alpha + \beta & = & \bigcup_{\gamma<\beta}(\alpha + \gamma) = \sup_{\gamma<\beta}(\alpha + \gamma), \ \beta \textit{ ordinale limite} \end{array}$$

Esempi 4.2.20. L'addizione tra numeri naturali, intesi come ordinali, ha tutte le consuete proprietà, ma di solito ciò non vale nel caso di ordinali infiniti (*transfiniti*): $1 + \omega = \omega$, $S(\omega) = \omega + 1 \neq \omega$.

La moltiplicazione $\alpha \cdot \beta$ di ordinali si può anch'essa definire in termini naturali, come addizione ripetuta:

$$\textit{contare } \alpha \textit{ per } \beta \textit{ volte}$$

usando l'insieme $\alpha \times \beta = \bigcup_{\delta<\beta} \alpha \times \{\delta\}$ ordinato con $<_{\alpha\cdot\beta}$, ottenuto facendo precedere ogni $\alpha \times \{\delta\}$ a $\alpha \times \{\delta'\}$ (ordinati entrambi secondo $\in_\alpha$, cioè $<_\alpha$) se $\delta <_\beta \delta'$. Quindi si definisce

Definizione 4.2.21 (Moltiplicazione ordinale)**.**

$$\alpha \cdot \beta = tipo(\alpha \times \beta; <_{\alpha\cdot\beta})$$

Direttamente da questa definizione si ottengono le caratteristiche fondamentali della moltiplicazione:

Teorema 4.2.22. *(Proprietà fondamentali della moltiplicazione ordinale) Se α, β, γ sono ordinali*

1. $(\alpha \cdot \beta) \cdot \gamma = \alpha \cdot (\beta \cdot \gamma)$

2. $\alpha \cdot 0 = 0 \cdot \alpha = 0$*,* $\alpha \cdot 1 = 1 \cdot \alpha = \alpha$

3. *Formule ricorsive per la moltiplicazione:*
$$\alpha \cdot \beta = \begin{cases} 0 & se \quad \beta = 0 \\ (\alpha \cdot \gamma) + \alpha & se \quad \beta \text{ è un ordinale successore, } \beta = S(\gamma) \\ \bigcup_{\gamma<\beta}(\alpha \cdot \gamma) & se \quad \beta \text{ è un ordinale limite, } \beta = \bigcup_{\gamma<\beta} \gamma \end{cases}$$
o, in termini più espliciti,
$$\begin{array}{lcl} \alpha \cdot 0 & = & 0 \\ \alpha \cdot (\gamma + 1) & = & (\alpha \cdot \gamma) + \alpha \\ \alpha \cdot \beta & = & \bigcup_{\gamma<\beta}(\alpha \cdot \gamma) = \sup_{\gamma<\beta}(\alpha \cdot \gamma),\ \beta \textit{ ordinale limite} \end{array}$$

4. $\alpha \cdot (\beta + \gamma) = (\alpha \cdot \beta) + (\alpha \cdot \gamma)$

Esempi 4.2.23. Anche la moltiplicazione tra numeri naturali, intesi come ordinali, ha tutte le consuete proprietà, ma di solito ciò non vale nel caso di ordinali infiniti (*transfiniti*): $2 \cdot \omega = \sup_{n<\omega}(2 \cdot n) = \omega$, ma $\omega \cdot 2 = \omega \cdot 1 + \omega =$ $= \omega + \omega$. In generale, $n \cdot \omega = \omega$ se $n \in \omega, n > 0$.
Anche

$$\omega \cdot \omega = (1 + \omega) \cdot \omega \neq (1 \cdot \omega) + (\omega \cdot \omega) = \omega + (\omega \cdot \omega).$$

Si è ora portati introdurre un elevamento a potenza che dia ad esempio $\omega \cdot \omega = \omega^2$, ma una definizione diretta è abbastanza complicata e poco 'naturale': è preferibile una definizione induttiva, basata su formule di ricorsione, che comunque segue l'idea di un elevamento a potenza come moltiplicazione ripetuta.

Definizione 4.2.24 (Elevamento a potenza ordinale)**.** Se α, β sono ordinali

$$\alpha^\beta = \begin{cases} 1 & \text{se} \quad \beta = 0 \\ (\alpha^\gamma) \cdot \alpha & \text{se} \quad \beta \text{ è un ordinale successore, } \beta = S(\gamma) \\ \bigcup_{\gamma<\beta}(\alpha^\gamma) & \text{se} \quad \beta \text{ è un ordinale limite, } \beta = \bigcup_{\gamma<\beta}\gamma \end{cases}$$

o, in termini più intuitivi,

$$\begin{aligned} \alpha^0 &= 1 \\ \alpha^{\gamma+1} &= (\alpha^\gamma) \cdot \alpha \\ \alpha^\beta &= \bigcup_{\gamma<\beta}(\alpha^\gamma) = \sup_{\gamma<\beta}(\alpha^\gamma),\ \beta\, \textit{ordinale limite} \end{aligned}$$

Come viene applicato qui il principio di induzione 4.2.14? Si definisce per ogni α fissato [5] mediante una formula una costruzione $\mathbf{F}_\alpha(x)$ per ogni x:

$$\mathbf{F}_\alpha(x) = \begin{cases} 0 & \text{se } x & \text{non è una funzione definita} \\ & & \text{su qualche ordinale } \beta \\ 1 & \text{se } x & \text{è la funzione vuota definita} \\ & & \text{su } \beta = 0 \\ x(\gamma) \cdot \alpha & \text{se } x & \text{è una funzione definita} \\ & & \text{sull'ordinale successore } \beta = S(\gamma) \\ \bigcup_{\gamma<\beta} x(\gamma) & \text{se } x & \text{è una funzione definita} \\ & & \text{sull'ordinale limite } \beta = \sup_{\gamma<\beta}(\gamma) \end{cases}$$

Esempi 4.2.25.

- Anche l'elevamento a potenza tra numeri naturali, intesi come ordinali, ha tutte le consuete proprietà delle potenze ordinarie (si noti che $0^0 = 1$).

- Come al solito ciò non vale però nel caso di ordinali transfiniti: $2^\omega = \sup_{n<\omega}(2^n) = \omega$, e in generale $n^\omega = \omega$ se $n \in \omega$, $n > 1$.

[5] Formalmente α è una variabile ordinale che vale da parametro per $\mathbf{F}$.

- Per ogni α valgono $\alpha^1 = \alpha$, $\alpha^2 = \alpha^{1+1} = \alpha \cdot \alpha$, $1^\alpha = 1$, ...

Una significativa applicazione 'elementare' dell'aritmetica ordinale è la rappresentazione posizionale di questi numeri, rappresentazione perfettamente analoga a quella dei numeri naturali, e dimostrabile nello stesso modo. Esponiamo solo il risultato fondamentale con alcune applicazioni, rimandando ad [Abian 1972, Cap.VIII, §7].

Come nel caso dei numeri naturali, si fissa un ordinale $\beta > 1$ (la *base*); le *cifre* della rappresentazione sono gli ordinali $\gamma < \beta$, cioè i $\gamma \in \beta$. Una *rappresentazione* di un ordinale $\alpha > 0$ in base β è uno sviluppo di α in una somma (finita) di $n > 0$ termini del tipo

$$\alpha = \sum_{j<n} \beta^{\varepsilon_j}\gamma_j = \beta^{\varepsilon_0}\gamma_0 + \ldots + \beta^{\varepsilon_{n-1}}\gamma_{n-1} \tag{4.2}$$

dove $\gamma_j \in \beta$ e gli ε_j sono ordinali, in ordine decrescente:

$$\varepsilon_0 > \varepsilon_1 > \ldots \geq \varepsilon_{n-1}$$

Le operazioni sono quelle dell'aritmetica ordinale, e perciò si deve rispettare l'ordine nelle somme e moltiplicazioni, non commutative.
Come si vede, c'è perfetta analogia con la consueta rappresentazione posizionale di un numero naturale, e il risultato fondamentale è lo stesso:

Teorema 4.2.26. *Ogni ordinale $\alpha > 0$ ha una unica rappresentazione posizionale in base $\beta > 1$, qualunque sia β.*

Dimostrazione. Vedi [Abian 1972, loc. cit., Teorema 32] □
Se α è rappresentato dallo sviluppo 4.2,

$$\alpha = \beta^{\varepsilon_0}\gamma_0 + (\ldots + \beta^{\varepsilon_{n-1}}\gamma_{n-1}) = \beta^{\varepsilon_0}\gamma_0 + \rho \tag{4.3}$$

ρ si dice il *resto*, mentre $\beta^{\varepsilon_0}\gamma_0$ è la *parte principale* dello sviluppo —la base elevata all'esponente massimo; γ_0 si dice la *cifra significativa* della rappresentazione.

Si può quindi rappresentare ogni $\alpha > 0$ in base 2:

$$\alpha = \sum_{j<n} 2^{\varepsilon_j} = 2^{\varepsilon_0} + \ldots + 2^{\varepsilon_{n-1}}, \quad \varepsilon_0 > \varepsilon_1 > \ldots \geq \varepsilon_{n-1}$$

in base 10, eccetera. Però risulta molto comoda per le operazioni con ordinali la *rappresentazione normale*, cioè in base ω:

$$\begin{aligned} &\alpha = \textstyle\sum_{j<n} \omega^{\varepsilon_j} m_j = \omega^{\varepsilon_0} m_0 + \ldots + \omega^{\varepsilon_{n-1}} m_{n-1}, \text{ con} \\ &m_j \in \omega, \quad \varepsilon_0 > \varepsilon_1 > \ldots \geq \varepsilon_{n-1} \end{aligned} \tag{4.4}$$

Esempio 4.2.27. Se $\alpha = \omega + 2$, le sue rappresentazioni in base 2 e rispettivamente normale sono:

$$\omega + 2 = 2^\omega \cdot 1 + 2^1 \cdot 1 = \omega^1 \cdot 1 + \omega^0 \cdot 2$$

con resti $\rho_2 = 2$ e $\rho_\omega = 2$. Le parti principali qui sono 2^ω e ω.

Con questa rappresentazione si ha anzitutto

Proposizione 4.2.28. *Se α ha la rappresentazione normale 4.4, è un successore se e solo se $\varepsilon_{n-1} = 0$.*

Dimostrazione. Vedi [Abian 1972, loc. cit., Lemma 22] □

Inoltre si hanno le seguenti regole di semplificazione:

$$\begin{aligned} n\omega^\varepsilon &= \omega^\varepsilon \\ \omega^{\varepsilon_1} m + \omega^{\varepsilon_2} n &= \omega^{\varepsilon_2} n, \ \varepsilon_1 < \varepsilon_2 \\ \omega^\varepsilon m + \omega^\varepsilon j &= \omega^\varepsilon (m + j) \\ (\omega^\varepsilon c + \rho) n &= \omega^\varepsilon c n + \rho \\ (\omega^\varepsilon c + \rho) \omega^\delta m &= \omega^{\varepsilon+\delta} m \\ (\omega^\varepsilon c + \rho)^\delta &= \omega^{\varepsilon+\delta} \end{aligned} \tag{4.5}$$

se gli ordinali ε, ε_1, ε_2, δ, sono > 0, e $c, m, j, n \in \omega$, $n > 0$.

Osservazioni 4.2.29.

- La prima equazione vale anche se ω^ε è rimpiazzato da un qualunque ordinale limite.

- Naturalmente, la terza equazione vale anche se $\varepsilon = 0$ o se m, j non sono numeri naturali; si tratta infatti di un caso particolare della distributività a destra della moltiplicazione.

- Le ultime tre equazioni si riferiscono a una rappresentazione normale con resto ρ, come in 4.2.

- Nell'ultima equazione δ è un ordinale limite.

Sulla base delle formule precedenti si possono eseguire molti calcoli con notevole semplicità.

Esercizi 4.2.30. Trovare le rappresentazioni normali di α, usando le equazioni 4.5 e le proprietà già viste, se

$\alpha = (2 \cdot \omega^{\omega+1} + \omega^2 \cdot 3) + (\omega^\omega + \omega + 2 \cdot \omega)$	Risposta:	$\omega^{\omega+1} + \omega^\omega + \omega \cdot 2$
$\alpha = (\omega^\omega \cdot 2 + \omega^2 + 1) \cdot (\omega^2 + 2)$	Risposta:	$\omega^{\omega+2} + \omega^\omega \cdot 4 + \omega^2 + 1$
$\alpha = (\omega^2 \cdot 3 + \omega)^2$	Risposta:	$\omega^4 \cdot 3 + \omega^3$
$\alpha = (\omega^2 + \omega + 1)^\omega$	Risposta:	ω^ω

4.3 I numeri cardinali

Possiamo ora definire con precisione l'idea di numero cardinale e quella di cardinalità di un insieme; per quest'ultimo aspetto è però indispensabile l'assioma di scelta. In una definizione o dimostrazione il suo uso è segnalato nel caso da (AS) premesso alle proposizioni relative. Per alcune notazioni, vedi Appendice A.3.2. Per la maggior parte delle dimostrazioni, il rinvio è ancora a [Kunen 1980, cap.1, §10] o a [Abian 1972, Cap.IX].

Definizioni 4.3.1.

- Dato un ordinale α, la sua cardinalità è il minimo ordinale β tale che $\beta \sim \alpha$: esso si indica con $|\alpha|$.

- Se $\alpha = |\alpha|$, esso si dice un (numero) cardinale.

- (AS) Se A è un qualsiasi insieme, la sua cardinalità, indicata con $card(A)$ o semplicemente con $|A|$, è quella di un qualunque ordinale simile ad A dotato di un qualsiasi buon ordinamento.

Osservazioni 4.3.2.

- Se α è un ordinale, la classe, non vuota, dei $\beta \sim \alpha$ ha minimo per il teorema 4.2.3, n.6: la classe in questione è però un insieme (vedi la proposizione 4.3.5).
- I numeri cardinali non sono che ordinali particolari: per distinguerli però dagli altri, li si indica con $\kappa, \lambda, \mu, \nu, \ldots$
- Tra i numeri cardinali in quanto ordinali è definita una relazione di $<$, coincidente con $\in$, che equivale a quella già definita per cardinalità (potenze) nelle definizioni 4.1.1. Valgono anche le proprietà della relazione di minore tra ordinali come casi particolari, a cominciare dalla legge di tricotomia per i cardinali: per le cardinalità di insiemi qualunque essa equivale ad AS ([Moore 1982, App.2, table 9]).
- I numeri naturali sono tutti numeri cardinali, e per ognuno non esistono altri ordinali ad esso equipotenti. ω è anch'esso un numero cardinale: è il minimo cardinale transfinito.
- È facile provare che anche $|A|$ è ben definito, qualunque sia l'insieme A (se vale AS). Infatti i buoni ordinamenti di A danno luogo a diversi tipi d'ordine, ma ovviamente questi sono tutti equipotenti tra loro.
- Valgono i teoremi già visti per le cardinalità (potenze) degli insiemi numerici (capitolo 1) e a proposito dell'assioma di scelta (sezione 3.2).

Vediamo ora alcuni risultati generali sui numeri cardinali.

Proposizione 4.3.3. *Se $\alpha \leq \beta$, risulta $|\alpha| \leq |\beta|$: quindi, se $|\alpha| \leq \beta \leq \alpha$, risulta $\alpha = \beta$.*

La dimostrazione è immediata dal teorema di Schröder-Bernstein. Una conseguenza importante è

Proposizione 4.3.4. *Se A è un insieme di cardinali $\sup(A) = \bigcup_{\kappa \in A} \kappa$ è un cardinale, il minimo cardinale $\geq$ di tutti i $\kappa \in A$.*

Dimostrazione. Sia $\alpha = sup(A)$: esso è un ordinale (proposizione 4.2.9) maggiore o uguale di ogni $\kappa \in A$: si ha quindi $|\alpha| \geq \kappa$ per la proposizione precedente. Se poi fosse $\alpha > |\alpha|$ si avrebbe $|\alpha| \in \bigcup_{\kappa \in A} \kappa$, da cui $|\alpha| < \kappa \leq |\alpha|$ per qualche $\kappa \in A$, da cui l'assurdo, e quindi deve essere $\alpha = |\alpha|$. È poi immediato mostrare che non può esistere un cardinale $\lambda < \alpha$ che sia maggiore o uguale di ogni $\kappa \in A$. □

Proposizione 4.3.5. *Dato un qualunque numero ordinale α, esiste un cardinale $\kappa > \alpha$.*

Dimostrazione. Basta provare questo per ordinali transfiniti. Si considerino i buoni ordinamenti R di α: essi costituiscono un insieme, dal momento che comunque $R \in \mathcal{P}(\alpha \times \alpha)$. Allora si può verificare che per rimpiazzamento

$$K = \{tipo(\alpha; R);\ R \text{ è un buon ordinamento di } \alpha\} = \{\beta;\ \beta \sim \alpha\}$$

è un *insieme* di ordinali, e che l'ordinale $sup(K)$ è il cardinale cercato. □

Osservazioni 4.3.6.

- Questa dimostrazione riprende e generalizza il metodo trovato da Cantor per costruire cardinali transfiniti, mediante *classi-numero*, gli insiemi –diremmo oggi– degli ordinali equipotenti al transfinito α. $sup\, K$ di fatto è il minimo cardinale maggiore di $|\alpha|$ (il successore cardinale di $|\alpha|$, definizione 4.3.7); più avanti (proposizione 4.3.19) proveremo che $|K| = sup\, K$, che è esattamente quanto trovato da Cantor. Vedi, per il caso più significativo, quello di $\alpha = \omega$, [Dauben 1979, pagg.202-09].

- È interessante notare che questo risultato non richiede AS, ma piuttosto l'assioma di rimpiazzamento, che qui è indispensabile.

- Come caso particolare si ottiene

  Dato un qualsiasi numero cardinale, ne esiste uno strettamente maggiore.

risultato che deriva anche dal teorema di Cantor sulla potenza 1.2.17, come questa proposizione, ma che richiede l'assioma di scelta per poter assegnare un cardinale all'insieme delle parti $\mathcal{P}(\alpha)$.

L'aritmetica cardinale è molto diversa da quella ordinaria e pure da quella ordinale, anche se nel caso dei numeri naturali non vi è alcuna differenza. Iniziamo con una nozione diversa di successore.

Definizione 4.3.7. Se κ è un numero cardinale, il minimo cardinale strettamente maggiore di esso è il suo successore cardinale (immediato): lo si indica con κ^+.

Questa volta, dato κ, la collezione dei numeri cardinali strettamente maggiori di esso è una classe propria, non vuota (proposizione precedente), e questo assicura l'esistenza del minimo.

I numeri naturali $\neq 0$ sono tutti successori (definizione 4.2.7), dato che il successore cardinale di un numero naturale m coincide col suo successore ordinale: $Sm = m^+$. Se però κ è transfinito, $S(\kappa) \sim \kappa$ e quindi $S(\kappa) < \kappa^+$: consideriamo perciò ora i soli cardinali transfiniti: anzitutto, dall'osservazione fatta sopra segue subito che

Proposizione 4.3.8. *Ogni cardinale transfinito è un ordinale limite.*

I cardinali transfiniti si possono ripartire in due classi, più ω:

Definizione 4.3.9. Se il cardinale $\kappa > \omega$ non è un successore, si dice un cardinale limite. Quindi ω, che non è un cardinale successore, non è nemmeno un cardinale limite.

La nozione di cardinale limite è diversa, come si vede, da quella di ordinale limite: ad esempio, ω è un ordinale limite che *non* è un *cardinale* limite, e si è visto che *tutti* i cardinali transfiniti sono ordinali limite, anche i successori.

Seguendo il simbolo attribuitogli da Cantor, ω, come primo cardinale transfinito, viene indicato con $\aleph_0$ 'alef zero': il simbolo $\aleph$ è la prima lettera dell'alfabeto ebraico, che viene usata per indicare gli ordinali transfiniti in generale.

Definizione 4.3.10. La *successione degli alef* è definita per ricorsione transfinita su tutti gli ordinali con

$$\begin{aligned} \aleph_0 &= \omega \\ \aleph_{\alpha+1} &= \aleph_\alpha^+ \\ \aleph_\alpha &= \bigcup_{\beta<\alpha} \aleph_\beta \text{ se } \alpha \text{ è un ordinale limite} \end{aligned}$$

Nell'ultimo caso $\aleph_\alpha$ è un cardinale, il minimo cardinale strettamente maggiore di ogni $\aleph_\beta$, $\beta < \alpha$ per la proposizione 4.3.4. Ecco alcune proprietà fondamentali della successione.

Proposizione 4.3.11.

1. *La successione degli alef è strettamente crescente:* $\forall\alpha\,\forall\beta\,(\alpha < \beta \Rightarrow \aleph_\alpha < \aleph_\beta)$.
2. *Se A è un insieme di ordinali,* $sup_{\alpha\in A}(\aleph_\alpha) = \aleph_{sup(A)}$
3. *Ogni cardinale transfinito è un (ben preciso) alef.*
4. $\aleph_\alpha$ *è un cardinale successore se e solo se α è un ordinale successore, ed è un cardinale limite se e solo se α è un ordinale limite.*
5. *I numeri cardinali transfiniti costituiscono una classe propria* **ALEF***; per conseguenza, anche tutti i cardinali sono una classe propria* **CARD**.

Dimostrazione.

1. La prima affermazione si prova direttamente per induzione tranfinita su β.
2. Sia $\beta = sup_{\alpha\in A}\alpha$: si tratta di provare che $sup_{\alpha\in A}(\aleph_\alpha) = \aleph_\beta$. Per 1, è comunque $sup_{\alpha\in A}(\aleph_\alpha) \le \aleph_\beta$; distinguiamo ora due casi.
   - β è il massimo di A. Allora, sempre per 1, il risultato è immediato.
   - β non è il massimo di A. Basta provare $sup_{\alpha\in A}(\aleph_\alpha) \ge \aleph_\beta$. Dato che $\forall\delta < \beta\,\exists\gamma \in A\ (\delta < \gamma < \beta)$, β è un ordinale limite (osservazione 4.2.13); per definizione allora $\aleph_\beta = sup_{\alpha<\beta}(\aleph_\alpha)$. Quindi
   $$\aleph_\beta = sup_{\delta<\beta}(\aleph_\delta) \le sup_{\gamma\in A}(\aleph_\gamma)$$

da cui l'uguaglianza cercata.

3. Sia κ un cardinale transfinito: possiamo supporre che sia $\kappa > \omega$. Consideriamo l'insieme A degli ordinali α tali che $\aleph_\alpha < \kappa$: A non è vuoto, dato che $0 \in A$; si ha $sup_{\alpha \in A}(\aleph_\alpha) = \aleph_\beta \leq \kappa$, se $\beta = supA$. Se vale $\aleph_\beta < \kappa$, segue $\beta \in A$ e non potrebbe essere $\aleph_{\beta+1} = \aleph_\beta^+ < \kappa$: quindi per tricotomia $\kappa = \aleph_{\beta+1}$. Altrimenti, $\aleph_\beta = \kappa$.

4. Se α è un ordinale successore, $\aleph_\alpha$ è un cardinale successore per definizione; anche il viceversa è immediato per quanto appena provato. La seconda parte dell'affermazione segue dalla prima.

5. **ALEF** è una classe propria perché in 'corrispondenza biunivoca' con **ORD**. □

4.3.1 L'aritmetica cardinale

Come si è anticipato, l'aritmetica cardinale differisce notevolmente da quella ordinale. Definiamo anzitutto addizione ($\oplus$) e moltiplicazione ($\otimes$) tra cardinali con simboli diversi per sottolineare la differenza.

Definizioni 4.3.12. Se κ e λ sono numeri cardinali

- $\kappa \oplus \lambda = |(\{0\} \times \kappa) \cup (\{1\} \times \lambda)|$
- $\kappa \otimes \lambda = |\kappa \times \lambda|$

Osservazioni 4.3.13.
- Nel caso della somma, come per quella ordinale, si ricorre all'artificio dell'unione disgiunta: vedi pagina 84.
- Queste definizioni non richiedono AS perché gli insiemi nella definizione sono bene ordinabili in maniera naturale: vedi la definizione delle analoghe operazioni ordinali in 4.2.1.
- Se κ, λ sono naturali, le due operazioni coincidono con la somma e il prodotto ordinari.

- Le due operazioni sono associative e commutative, dotate di elemento neutro.

Si possono applicare le definizioni precedenti di somma e prodotto cardinali al caso di insiemi qualunque, ma si richiede l'assioma di scelta:

Proposizione 4.3.14. *(AS) Se A, B sono insiemi qualunque, risulta*

- $|A| \oplus |B| = |(\{0\} \times A) \cup (\{1\} \times B)|$
- $|A| \otimes |B| = |A \times B|$

Quando però si hanno cardinali infiniti, queste operazioni hanno un risultato non ovvio, anche se in qualche modo banale [Kunen 1980, cap.1, §10.13]:

Teorema 4.3.15. *Se uno dei due cardinali, ad esempio κ, è infinito, si ha*

- *$\kappa \oplus \lambda = max\{\kappa; \lambda\}$ e anche*
- *$\kappa \otimes \lambda = max\{\kappa; \lambda\}$, purché $\lambda \neq 0$*
- *(AS) Stessa conclusione per cardinalità $|A| = \kappa$ e $|B| = \lambda$ di insiemi qualunque*

Questo risultato generalizza il corollario 1.2.14 relativo all'unione di un insieme numerabile con uno più che numerabile. Vediamone qualche altra conseguenza.

Corollario 4.3.16. *(AS) Se $|A|$ è infinito e $n \in \omega$, $n \neq 0$, $|A^n| = |A|$.*

A^n è qui il prodotto cartesiano di A per se stesso n volte.

Più interessante è un risultato sulle unioni.

Teorema 4.3.17. *(AS) Se κ è infinito e $\mathcal{A} = \{X_\alpha; \alpha \in \kappa\}$ con $|X_\alpha| \leq \kappa$ per ogni $\alpha \in \kappa$, allora $|\bigcup \mathcal{A}| = |\bigcup_{\alpha<\kappa} X_\alpha| \leq \kappa$.*

A parole, questo risultato si può enunciare così:

Se κ è infinito, l'unione di una famiglia di cardinalità $\leq \kappa$ di insiemi, tutti di cardinalità $\leq \kappa$, ha ancora cardinalità $\leq \kappa$.

Questo risultato estende dal caso $\kappa = \omega$ a tutti i cardinali transfiniti il teorema dell'unione numerabile 3.2.20, e si dimostra sostanzialmente nello stesso modo, sostituito κ a ω e tenuto conto che $\kappa \otimes \kappa = \kappa$. Infine, il risultato

sulle somme di cardinali transfiniti permette di giustificare la costruzione del successore di un alef in termini di classi-numero, come già accennato nelle osservazioni 4.3.6. Anzitutto, una definizione precisa.

Definizione 4.3.18. $\mathbf{Z}(\aleph_\beta) = \{\alpha;\ \alpha \sim \aleph_\beta\}$ si dice la classe-numero di $\aleph_\beta$ (è però un insieme).

Si ha subito, riprendendo la dimostrazione della proposizione 4.3.5:

Proposizione 4.3.19. $\mathbf{Z}(\aleph_\beta)$ *ha cardinalità* $\aleph_\beta^+ = \aleph_{\beta+1}$.

Dimostrazione. Usiamo i simboli della dimostrazione menzionata. Se $|\alpha| = \aleph_\beta$, l'insieme K è l'insieme $\mathbf{Z}(\aleph_\beta)$: allora il cardinale $sup(K)$ è il suo successore $\aleph_\beta^+$. Poiché $\aleph_\beta^+ = K \cup \aleph_\beta = K \cup |\alpha|$, insiemi disgiunti, si ha $|K| = \aleph_\beta^+$, cioè la tesi. $\square$

L'operazione più caratteristica dell'aritmetica cardinale è l'elevamento a potenza. Essa è completamente diversa dalla analoga operazione ordinale.

Definizione 4.3.20. (AS) Se κ, λ sono cardinali κ^λ è $|F(\lambda;\, \kappa)|$. L'assioma di scelta è indispensabile per assicurare un buon ordinamento per $F(\lambda;\, \kappa)$, l'insieme delle funzioni $f : \lambda \longrightarrow \kappa$. Naturalmente, se A, B sono insiemi, valendo AS, si ha $|A|^{|B|} = |F(B; A)|$.

Questa definizione generalizza la legge combinatoria, valida nel finito, sulle disposizioni con ripetizione: in effetti, se k, $m \in \omega$, k^m è il numero di funzioni $f : m \longrightarrow k$, se si tiene presente che k ha k elementi, e così via: k^m ha insomma lo stesso valore in tutti i casi (aritmetico, ordinale, cardinale). $0^0 = 1$ ha però *un* elemento, la funzione biunivoca (!) vuota...

Esempi 4.3.21. $0^\kappa = 0$ (se $\kappa \neq 0$); $\forall \kappa$, $1^\kappa = 1$; $\kappa^0 = 1$, $\kappa^1 = \kappa$. Come prima, anche interpretando κ^n come la cardinalità di $F(n;\kappa)$ si ha, se κ è infinito e $n > 0$, $\kappa^n = \kappa$. Se vale AS, lo stesso si applica a $|A| = \kappa$, qualunque sia A.

Un risultato notevole è quello relativo all'insieme potenza:

Proposizione 4.3.22. *(AS) Per ogni insieme A, $|\mathcal{P}(A)| = 2^{|A|}$.*

Dimostrazione. Se $B \subseteq A$, lo si può identificare con la sua funzione caratteristica χ_B di dominio A: poiché $2 = \{0;1\}$, ciò crea una corrispondenza biunivoca di $\mathcal{P}(A)$ con $F(A;2)$. $\square$

Anche questo risultato generalizza nell'infinito un risultato combinatorio: se A ha n elementi, $\mathcal{P}(A)$ ne ha 2^n, e questo dà il nome alternativo di 'potenza' all'insieme delle parti.

Osservazione 4.3.23. L'elevamento a potenza si indica nello stesso modo sia nel caso ordinale che nel caso cardinale, ma i risultati, se almeno uno dei due numeri coinvolti è infinito, possono essere ben diversi. Non c'è pericolo di confusione se si indicano cardinali o ordinali con lettere greche differenti, o se per i cardinali si usano i segni di valor assoluto o gli alef, ma in alcuni casi bisogna ben distinguere: sebbene in senso ordinale $2^\omega = \omega$ (esempi 4.2.25) e $\omega = \aleph_0$, in senso cardinale $2^{\aleph_0} = \mathfrak{c} = |\mathbb{R}|$, che è un cardinale ben diverso (proposizione 1.2.16).

Per la cardinalità di $\mathbb{R}$ (la *potenza del continuo*, nella terminologia di Cantor) si è introdotto un simbolo apposito, $\mathfrak{c}$: essendo un cardinale transfinito, esso deve essere un alef —ma quale? Si è visto che questo problema è all'origine dell'ipotesi del continuo (sezione 3.3) e che nemmeno in ZFC, in cui si può ottenere un buon ordinamento di $\mathbb{R}$, si può risolvere questo interrogativo. Possiamo ora formulare CH e GCH in termini degli alef.

Ipotesi del continuo, **CH**	Ipotesi generalizzata del continuo, **GCH**
$2^{\aleph_0} = \aleph_1$	$\forall \alpha, \qquad 2^{\aleph_\alpha} = \aleph_{\alpha+1}$

Vediamo infine le prime 'regole di calcolo' con gli esponenti cardinali; è interessante osservare che quelle consuete per gli esponenti valgono ancora:

Teorema 4.3.24. *Se κ, λ, μ sono numeri cardinali,*

$$\kappa^{\lambda \oplus \mu} = \kappa^{\lambda} \otimes \kappa^{\mu} \text{ e } \kappa^{\lambda \otimes \mu} = (\kappa^{\lambda})^{\mu}$$

Se vale AS, dati insiemi A, B, C si ha analogamente

$$|A|^{|B| \oplus |C|} = |A|^{|B|} \otimes |A|^{|C|} \text{ e } |A|^{|B| \otimes |C|} = (|A|^{|B|})^{|C|}$$

Dimostrazione. Dimostriamo queste regole direttamente per insiemi A, B, C con corrispondenze biunivoche.

- Nel primo caso si tratta di provare che, se B e C sono disgiunti,

  $$F(B \cup C; A) \sim (F(B; A) \times F(C; A))$$

  La corrispondenza biunivoca 'naturale' è, in questo caso,

  $$f \in F(B \cup C; A) \mapsto (f \restriction B \,; f \restriction C) \in (F(B; A) \times F(C; A)).$$

- Nel secondo caso si deve invece provare che

  $$F(B \times C; A) \sim F(C; (F(B; A)))$$

  La corrispondenza biunivoca 'naturale' è allora

  $$f(\cdot \,; \,\cdot) \in F(B \times C; A) \mapsto (y \in C \mapsto f(\cdot \,; y) \in F(B; A)).$$

Capitolo 5

Varianti di ZF e teorie alternative

Nell'àmbito di ZF si può estendere la portata del concetto di insieme in diverse direzioni. Già abbiamo visto che è permesso rappresentare con particolari insiemi l'ordine di presentazione degli elementi mediante l'assioma della coppia, il concetto di coppia ordinata e quello di relazione.

Anche la 'molteplicità di appartenenza' di un elemento a un insieme (si pensi alle soluzioni di un'equazione algebrica) si può rendere facilmente: si ha la definizione di *multiinsieme*, che è una coppia $(a; f)$, dove a è un insieme e $f : a \to \mathbb{N}^+$; intuitivamente $f(x)$ è appunto la molteplicità di appartenenza di x ad a.

In fondo simile è la definizione di *fuzzy set* ('insieme sfumato'), o meglio di sottoinsieme sfumato b di un insieme a: identificati i sottinsiemi classici con le loro funzioni caratteristiche, è poi naturale considerare funzioni $f_b : a \to [0; 1]$ e chiamarle (identificarle con) sottoinsiemi sfumati b di a. $f_b(x)$ rappresenta il grado di appartenenza di x a b e questa funzione viene considerata come sottoinsieme *sfumato* b di a: $f_b(x) = 0$ vale "x non appartiene in nessun modo a b", $f_b(x) = 1$ vale "x appartiene certamente a b". Non si dovrebbe confondere f_b con una probabilità: si pensi piuttosto a una nozione sfumata come 'essere alto', che determina, in un insieme di persone, un corrispondente sottoinsieme sfumato.

5.1 Assiomi alternativi in ZF

5.1.1 Insiemi non ben fondati e Antifondazione

Il fatto notevole che l'assioma di regolarità, che implica la buona fondazione di tutti gli insiemi in ZF, non sia necessario alla matematica, suggerisce che si potrebbe operare non solo in assenza di esso, ma anche con qualche forma della sua negazione, che indichi quali insiemi possono essere considerati non ben fondati senza contraddizioni: certamente tutti gli ordinali sono ben fondati per definizione, ma possiamo pensare all'utilità di insiemi del genere in alcuni casi.

In effetti, talvolta l'assioma di fondazione può ostacolare una impostazione insiemistica intuitiva: per fare un esempio significativo proprio perché banale, nel calcolo delle probabilità, quando schematizziamo un evento come insieme di casi elementari, dobbiamo distinguere forzatamente tra un caso elementare c e l'evento $\{c\}$ che si verifica solo per c, altrimenti si avrebbe $c \in \{c\} = c$.

Ma vari problemi sorgono immediatamente quando si ammette l'esistenza di insiemi non ben fondati: quali possono essere usati senza ottenere contraddizioni? Quanti elementi avrebbe un tale insieme, diciamo un a tale che $a = \{a; \{a\}\}$? Recentemente (1981) è stato introdotto da P. Aczel un assioma che permette in maniera costruttiva di utilizzare anche insiemi non ben fondati, utili in diverse applicazioni all'informatica ed alle scienze umane. Per maggiori dettagli si può leggere l'articolo divulgativo [Barwise-Moss 1991].

5.1.2 Proposizioni alternative all'assioma di scelta

Sono stati proposti molti assiomi che negano la validità assoluta di AS, o più modestamente, proposizioni incompatibili con esso. Ad esempio (per una ampia discussione, vedi [Moore 1982]):

- $\mathbb{R}$ è una unione numerabile di insiemi numerabili (E. P. Specker, in [Moore 1982, 5.1]);

- P. J. Cohen ha provato che esistono modelli di ZF in cui $\mathbb{R}$ non può essere bene ordinato, e quindi questa affermazione è una alternativa (consistente con ZF) ad AS [Moore 1982, 5.2].

5.1.3 Proposizioni alternative all'ipotesi del continuo

Attualmente, dopo la prova che l'ipotesi del continuo è indipendente da ZFC, si tende a studiarne qualche forma alternativa, che ammetta, o almeno sia compatibile con l'esistenza di cardinali κ intermedi tra $\aleph_0$ e $2^{\aleph_0}$, ma che al tempo stesso assicuri che questi cardinali non differiscano troppo da $\aleph_0$ stesso: quindi un indebolimento più che una alternativa all'ipotesi del continuo.

Un enunciato, deducibile da $ZFC \cup \{CH\}$ ma consistente in ZFC con $\neg CH$, che viene molto studiato è l'Assioma di Martin (MA) [1] , che si può enunciare come proposizione di topologia generale così (vedi [Kunen 1980, cap.II, §2], anche per le nozioni di topologia connesse):

Assioma di Martin [MA]
Siano $\aleph_0 \leq \kappa < 2^{\aleph_0}$, X uno spazio topologico compatto di Hausdorff che soddisfi la condizione della catena numerabile: allora X non può essere l'unione di κ chiusi mai densi F_α di X $(\alpha < \kappa)$

La condizione delle catene numerabili (c.c.c., *countable chain condition*) significa che le famiglie di aperti disgiunti di X sono al più numerabili.
Si ottengono da MA per i cardinali κ, $\aleph_0 \leq \kappa < 2^{\aleph_0}$ numerosi risultati, indipendenti da $ZFC \cup \{\neg CH\}$. Ad esempio:

- $2^\kappa = 2^{\aleph_0}$
- L'unione di κ sottoinsiemi di $\mathbb{R}$ di misura nulla secondo Lebesgue ha misura nulla.

Nonostante queste plausibili conseguenze, MA non è di certo 'intuitivamente plausibile' come gli assiomi di ZF: è scaturito piuttosto da problemi tecnici legati ai metodi introdotti da P. J. Cohen.

[1] D. A. Martin e R. M. Solovay, 1970.

5.1.4 Enunciati indipendenti da ZFC

Molti problemi aperti di topologia della retta reale si sono rivelati irrisolvibili in ZFC. A quelli precedenti si possono aggiungere l'ipotesi di Suslin e quella di Borel.

Questa congettura [2] deriva dai tentativi di caratterizzare la topologia ordinaria dei numeri reali in termini della struttura d'ordine $(\mathbb{R}; <)$: Suslin provò che ogni spazio topologico X, dotato della topologia determinata da un ordine totale tale che risulti

(i) X non ha né primo né ultimo elemento;

(ii) X è connesso nella topologia dell'ordine;

(iii) X è separabile nella stessa topologia

risulta isomorfo come insieme ordinato (e quindi omeomorfo come spazio topologico) a $\mathbb{R}$. Suslin si chiese se era possibile sostituire in questa caratterizzazione la separabilità con (iii'): la c.c.c. Se vale la

Ipotesi di Suslin, SH
Non esistono spazi topologici S con la topologia data da un ordine totale che soddisfino la condizione della catena numerabile ma che *non* siano separabili

chiaramente la nuova caratterizzazione è equivalente alla prima. Viceversa, se SH non vale, cioè se esiste uno spazio S totalmente ordinato c.c.c. ma non separabile (una *retta di Suslin*), ve ne sono anche altri che soddisfano le condizioni i e ii. Quindi SH è equivalente all'affermazione che i-ii-iii' caratterizzano la topologia di $\mathbb{R}$ data dagli intervalli.

SH risulta indipendente da $ZFC \cup \{CH\}$ (in particolare,consistente con esso); essa segue in ZFC da $MA \cup \{\neg CH\}$. Vedi [Kunen 1980, cap.II, §4], [Andretta 2003, I parte].

[2] M. Ya. Suslin, 1920.

Un'altra proposizione indipendente da ZFC è la congettura di Borel (BC) legata alla teoria della misura. Anzitutto,

Definizione 5.1.1. Un sottoinsieme X di $\mathbb{R}$ è di misura fortemente nulla se, data una qualsiasi successione infinitesima di numeri $\varepsilon_n > 0$, si possono trovare intervalli aperti I_n, ognuno di lunghezza $< \varepsilon_n$, che ricoprono X.

È immediato che un insieme di misura fortemente nulla è di misura nulla nel senso ordinario; il viceversa non vale, e un controesempio è dato dall'insieme ternario di Cantor (teorema 1.2.15): lo si può provare per esercizio. Ogni insieme (al più) numerabile è però fortemente di misura nulla: basta ricoprire ogni suo elemento x_n con l'intervallo $]x_n - \frac{\varepsilon_n}{3}; x_n + \frac{\varepsilon_n}{3}[$. Borel congetturò che questa fosse l'unica possibilità:

Congettura di Borel, BC
Ogni $X \subset \mathbb{R}$ di misura fortemente nulla è al più numerabile

BC è indipendente da ZFC, ma se si ammette CH si può dimostrare che BC non è vera: $ZFC \vdash CH \Rightarrow \neg BC$.

Attualmente la ricerca sui fondamenti concerne molto spesso lo studio di molti di questi risultati di indipendenza, consistenza relativa e derivabilità o refutabilità: vedi [Andretta 2003], [Kunen 1980].

Vediamo ora alcune teorie che differiscono in varia misura da ZF: esse descrivono variazioni della stessa idea di collezione matematicamente rilevante che dà luogo alla teoria degli insiemi, ma in maniera diversa rispetto all'ordinario.

5.2 La teoria delle classi NBG

Si è già detto cosa si intenda per classe; è possibile per esse trovare assiomi che non portino a contraddizioni. La teoria NBG è fondamentalmente simile a ZF: semplicemente, un insieme viene considerato come una classe che è elemento di qualche altra classe, e i risultati per questi ultimi sono equivaleni a quelli di ZF. Si parla di teoria *NBG* (Von Neumann-Bernays-Gödel).

NBG permette di trattare in maniera più vicina all'intuizione anche casi che in ZF *non* corrispondono a relazioni o funzioni, perché si otterrebbero classi proprie come estensione. Si è già visto che, ad esempio, l'inclusione tra insiemi non costituisce una relazione nel senso di '*insieme* di coppie' che il termine ha in ZFC; non si può definire in ZFC una *funzione* potenza $A \mapsto \mathcal{P}(A)$, sebbene questa costruzione sia relativa a un simbolo funzionale ben definito, eccetera: però in NBG l'inclusione tra insiemi [3] è chiamata relazione a pieno titolo, così come $\mathcal{P}$ è una funzione.

Descriviamo brevemente gli assiomi di NBG seguendo [Mendelson 1972, cap.4]. Il linguaggio comprende tra i simboli propri un solo simbolo predicativo binario infisso $\in$; le variabili (*variabili per classi*) si indicano tradizionalmente con lettere maiuscole: $X_1, X_2, \ldots$, variabili generiche con $X, Y, Z, \ldots$ senza indici. L'uguaglianza viene *definita* usando il principio di estensionalità per classi:

$$X \equiv Y \Leftrightarrow \forall Z\,(Z \in X \Leftrightarrow Z \in Y)$$

ma questo non è essenziale, anche se permette di vedere NBG come teoria finitamente assiomatizzata: l'assioma di estensione diventa ora

Assioma di estensione per NBG [E]
Date due classi X e Y, se $X \equiv Y$, X e Y appartengono alle stesse classi
$X \equiv Y \Rightarrow \forall Z\ (X \in Z \Leftrightarrow Y \in Z)$

L'assioma è indispensabile per provare che $\equiv$ è effettivamente di uguaglianza: a sua volta, ciò permette di usare il *classificatore* $\{x;\ \ldots\}$ per descrivere una classe, dopo averne provata l'esistenza.

Caratteristica è invece, come si è detto, la *definizione* di insieme, mediante un nuovo predicato 1-ario M, come di una classe tanto ristretta da poter

[3] Si noti che l'inclusione si può definire tra due classi qualunque, ma come classe di coppie ordinate è una relazione tra *insiemi*: vedi l'osservazione 5.2.1 a proposito delle coppie.

essere pensata come 'un tutto unico', secondo la definizione di Cantor stesso, in quanto possibile elemento di altra classe:

$$M(X) \Leftrightarrow \exists Y(X \in Y)$$

Una classe propria X sarà allora una classe per cui vale $\neg M(X)$. Si potrebbero usare quantificazioni limitate per insiemi, ma si usano invece solitamente, con lo stesso significato, lettere *minuscole* $x_1, x_2, \dots$ (e $x, y, z, \dots$ per variabili generiche). Vengono poi dati assiomi che assicurano l'esistenza dell'insieme vuoto e delle coppie non ordinate.

Assioma dell'insieme vuoto per NBG [V]
Esiste un insieme che non ha elementi

Assioma della coppia per NBG [C]
Dati insiemi x, y esiste un insieme che ha per unici elementi x e y

Osservazioni 5.2.1.

- V permette la definizione (al solito corretta per l'unicità garantita dall'assioma di estensione) di $\emptyset$. Esso non è indipendente dagli altri assiomi, lo si potrebbe ricavare dai seguenti, essenzialmente dall'assioma dell'infinito, l'unico altro assioma di esistenza per insiemi in NBG (vedi sotto), ma è opportuno inserirlo a questo punto, perché permette di snellire la trattazione seguente.

- C permette di introdurre coppie, non ordinate e poi ordinate, nel solito modo. Se si vuole che la costruzione di coppia non ordinata determini una funzione nel senso di NBG, occorre però definire $\{X; Y\}$ per tutte le classi X, Y; se esse sono entrambi insiemi l'assioma di estensione garantisce l'unicità; se X e Y non sono entrambi insiemi, si conviene che $\{X; Y\} = \emptyset$, di modo che le coppie non ordinate sono sempre insiemi.

- Le coppie e le n-uple ordinate di *insiemi* si introducono poi nel solito modo.

Seguono poi gli *assiomi delle classi*, in numero finito, che dicono quali fbf fondamentali definiscono classi per comprensione: li enunciamo informalmente.

Assiomi delle classi per NBG [CL1-CL7]
(CL1-Assioma della relazione $\in$) Esiste una classe X che ha come elementi le coppie ordinate $(x; y)$ di insiemi x, y tali che $x \in y$.
(CL2-Assioma dell'intersezione) Date due classi X e Y, esiste una classe Z che ha per elementi gli insiemi che appartengono sia ad X che ad Y.
(CL3-Assioma del complementare) Data una classe X, il suo complementare X' è una classe, definita da $\forall z(z \in X \Leftrightarrow z \notin X')$.
(CL4-Assioma del dominio) Per ogni classe X, esiste una classe Z costituita dalle prime componenti u delle coppie $(u; v) \in X$.
(CL5-Assioma della retroproiezione) Per ogni classe X, esiste una classe Z costituita dalle coppie $(u; v)$ con $u \in X$.
(CL6-Assioma della permutazione ciclica) Per ogni classe X, esiste una classe Z costituita dalle terne $(u; v; w)$ con $(v; w; u) \in X$.
(CL7-Assioma della trasposizione) Per ogni classe X, esiste una classe Z costituita dalle terne $(u; v; w)$ con $(u; w; v) \in X$.

Nell'ottica di ZF, si tratta spesso di classi proprie. Come applicazione, si possono ad esempio introdurre la classe universale di Cantor come complemento di $\emptyset$, l'unione booleana tra due classi, eccetera.

Soprattutto però questi assiomi determinano delle fbf alle quali è possibile applicare il principio di comprensione senza (si spera) contraddizioni: sono le fbf *predicative* del linguaggio.

Definizione 5.2.2. Sia $\phi = \phi(^n X; {}^k Y)$ una fbf del linguaggio con variabili libere comprese tra quelle scritte. Se in essa compaiono (al più) quantificazioni relative a variabili di insieme, una tale fbf si dice predicativa.

Teorema 5.2.3. [Mendelson 1972, prop. 4.4] *Se $\phi = \phi(^n X; {}^k Y)$ è predicativa, esiste una classe Z i cui elementi sono le n-uple $^n x$ tali che vale $\phi(^n x; ^k Y)$, cioè $Z = \{^n x;\ \phi(^n x; ^k Y)\}$.*

Le solite costruzioni insiemistiche sono permesse da assiomi analoghi a quelli di ZF, ma con un differente significato: consideriamo infatti l'assioma dell'unione e quello della potenza. Se si ha una classe X qualunque, possiamo ottenere la classe $\bigcup X$ degli (insiemi) elementi di elementi di X; le sue sottoclassi che sono insiemi sono gli elementi di un'altra classe precisa $\mathcal{P}(X)$, ben definibile anch'essa mediante una fbf predicativa (quali?). Gli assiomi dell'unione e della potenza ci assicurano allora che, se X è un insieme, lo sono anche le relative classi unione di X e potenza di X.

Assioma dell'unione per NBG [U]
$\bigcup X = \bigcup_{x \in X} x$ è un insieme se lo è X

Assioma della potenza per NBG [P]
$\mathcal{P}(X) = \{x; x \subseteq X\}$ è un insieme se lo è X

Per enunciare il seguente assioma di rimpiazzamento, occorre introdurre classi univoche:

$$Un(X) \Leftrightarrow (\forall x \forall y \forall z((x; y) \in X \wedge (x; z) \in X \Rightarrow x \equiv z)$$

cioè X è univoca quando, contenendo due coppie ordinate con prima componente uguale, le seconde componenti devono coincidere anch'esse. Enunciamo insieme anche un assioma (a rigore superfluo) che rimpiazza lo schema di specificazione di ZF.

Assioma di specificazione per NBG [S]
L'intersezione tra una classe Y e un insieme x è un insieme.

Assioma di rimpiazzamento per NBG [R]
Data una classe univoca X, se le prime componenti delle sue coppie sono ristrette a variare in un insieme x, anche le relative seconde componenti costituiscono un insieme.

Osservazioni 5.2.4.

- Segue subito da S che una sottoclasse di un insieme è un insieme. Questo assioma è tuttavia una conseguenza del più potente assioma (non schema) di rimpiazzamento. Dati x e Y, basta considerare la classe X delle coppie $(u;u)$ con $u \in Y$, definibile con la fbf predicativa $\phi(z;Y)$: $\exists u_1 \exists u_2 (z = (u_1;u_2) \wedge u_1 \equiv u_2 \wedge u_1 \in Y)$. Evidentemente $Un(X)$. Se le prime componenti delle sue coppie variano in x le seconde costituiscono $x \cap Y$, che è dunque un insieme per rimpiazzamento. Si noti l'analogia coi corrispondenti schemi di ZF.

- Sia nel caso di S che in quello di R, nel passaggio da ZF a NBG gli schemi divengono singole fbf giacché in quest'ultimo sistema si può quantificare su classi, che venivano in ZF rappresentate da fbf.

Infine, l'assioma dell'infinito si enuncia esattamente come in ZF. Per discuterlo meglio, vediamone anche la versione formale.

Assioma dell'infinito per NBG [I]
Esiste un insieme induttivo
$\exists x(\emptyset \in x \wedge \forall u(u \in x \Rightarrow u \cup \{u\} \in x))$

Questo è l'unico assioma di esistenza per un insieme: da esso allora si può dedurre l'esistenza di $\emptyset$, ma bisogna riformulare l'assioma I stesso, rimpiazzando l'insieme vuoto con una sua definizione. Anziché $\emptyset \in x$ si inserisce allora in I la fbf $\exists u(u \in x \wedge \forall z(z \notin u))$.

È chiaro come dagli assiomi E, C, R, CL1-CL7, U, P, I limitandosi agli insiemi si possa ricavare ZF (S, V si derivano da questi). Questi costituiscono la teoria NBG, che è finitamente assiomatizzata, a differenza di ZF.

Osserviamo come in NBG vengano evitati i paradossi, ad esempio quello di Russell. La classe di Russell R è ben definita, giacché $x \notin x$ è predicativa. Dunque $\forall X(M(X) \Rightarrow (X \in R \Leftrightarrow X \notin X))$. Supponiamo $M(R)$: allora $R \in R \Leftrightarrow R \notin R$ e quindi, data la contraddizione, $\neg M(R)$. Quindi in NBG i paradossi divengono dimostrazioni del fatto che certe classi sono proprie.

5.3 La teoria interna degli insiemi IST

Descriviamo con qualche dettaglio la IST (acronimo per 'Internal Set Theory') di E. Nelson, meno nota e più distante dall'idea che ordinariamente ci si fa di insieme. Per questa sezione rimandiamo a [Robert 1988].

5.3.1 Gli assiomi di IST

In questa teoria si introducono:

- L'usuale linguaggio della teoria degli insiemi (simboli propri: $=$, $\in$), le consuete fbf (dette 'interne' oppure 'classiche') e i consueti assiomi di ZFC [4]. Tutto ciò che è formulabile o dimostrabile in quest'àmbito si dirà *classico*.

- Un nuovo simbolo di predicato ad un posto, o proprietà, St: $St(a)$ ha il significato intuitivo "a è un oggetto (insieme, elemento,...) standard, accessibile...". I quantificatori limitati a questa proprietà si indicano così: "per ogni y standard" si abbrevia con $\forall^{st} y$, eccetera. Per variabili standard si intendono appunto quelle da quantificare (universalmente, se sono libere, per ottenere degli enunciati) con questa limitazione, oppure da sostituire con termini standard.

- Tre nuovi assiomi (denominazione corrente: in realtà, schemi), che descrivono l'uso corretto di St: li esponiamo in modo semi-formale.

Schema di idealizzazione per IST [I]
Se $\phi = \phi(x; y)$ è una fbf interna, sono equivalenti: i) per ogni a finito e standard, esiste un $x = x_a$ tale che $\phi(x; y)$ vale per ogni $y \in a$; ii) esiste un x tale che $\forall^{st} y\, \phi(x; y)$.
In ϕ possono comparire altre variabili libere, tranne a

[4] Negli schemi di specificazione e rimpiazzamento si ammettono solo fbf interne.

Osservazione 5.3.1. Si indica con $\mathbb{N}$ l'insieme dei numeri naturali di IST, che comprende anche numeri non standard, come si vedrà in séguito. Un insieme a è finito in IST se, come al solito, si può mettere in corrispondenza biunivoca con insiemi del tipo $\{m \in \mathbb{N}; m < j\}$ con $j \in \mathbb{N}$: è una proprietà classica (simbolo: $Fin(a)$, una fbf interna). Dunque questi insiemi in IST possono avere caratteristiche assai diverse dagli insiemi finiti usuali: tuttavia un insieme è finito e standard se e solo se ha tutti gli elementi standard, e si ritrovano gli insiemi finiti ordinari (vedi sotto, proposizione 5.3.6).

Schema di standardizzazione per IST [S]
e sia un insieme standard e $\phi = \phi(x)$ una fbf (anche non classica): esiste un (unico) sottoinsieme standard a di e tale che gli elementi standard di a sono esattamente gli $x \in e$ standard per cui vale ϕ.
Al solito, possono comparire in ϕ altre variabili libere, tranne a

Notazioni: a, la *parte standard* di e, si indica con $\{x \in e; \phi(x)\}^{st}$.

Schema di trasferimento per IST [T]
ψ sia una formula interna in cui compaiano libere, oltre a x, al più delle variabili standard ${}^m u$: allora $\forall x\, \psi(x;\ {}^m u) \ \Leftrightarrow\ \forall^{st} x\, \psi(x;\ {}^m u)$.

Naturalmente vi è una versione esistenziale equivalente T' di T: $\exists x \psi(x;\ {}^m u) \ \Leftrightarrow\ \exists^{st} x \psi(x;\ {}^m u)$

Osservazione 5.3.2. Segue che, se $\psi(x;\ {}^m u)$ vale per un unico x, esso è necessariamente standard.

5.3.2 Alcune conseguenze, più o meno strane, di IST

Vediamo ora alcune conseguenze degli schemi I, S e T; per quanto paradossali, esse riflettono la nozione di insieme che si vuole precisare: una collezione sulla quale possiamo avere una chiara percezione soltanto per porzioni finite sebbene ampliabili indefinitamente. Gli elementi non standard sono una sorta di 'elementi all'infinito' postulabili ma non effettivamente afferrabili, idea che si trova all'origine di molte costruzioni matematiche.

Osserviamo anzitutto che, in base a T, ogni insieme ben definibile classicamente a partire da insiemi standard è standard.

Esempi 5.3.3.
- Lo sono $\emptyset$, $\{0\} = 1$, $\{0;1\} = 2$,... Ad esempio, dato che esiste un solo x tale che $\forall\, z(z \notin x)$ —l'insieme vuoto— applicando T a questa *fbf* interna si ha che $\emptyset$ è standard.
- Analogamente, l'unione di due insiemi standard u_1, u_2 è standard —si usi la *fbf* interna $\forall\, z(z \in x \Leftrightarrow z \in u_1 \vee z \in u_2)$, e così via.

Una conseguenza importante di T è ancora questa generalizzazione del principio di estensione:

Proposizione 5.3.4. *Due insiemi standard a, b sono uguali se e solo se hanno gli stessi elementi* standard.

Dimostrazione. Si usi T sulla formula $\forall^{st} x(x \in a \Leftrightarrow x \in b)$. □
Analogamente, sempre se a, b sono standard, $a \subseteq b$ se e solo se ogni $x \in a$ standard è elemento di b, in base alla formula $\forall^{st} x(x \in a \Rightarrow x \in b)$.

Corollario 5.3.5. *La parte standard, la cui esistenza è garantita da S, è unica, come conseguenza di T.*

Vediamo ora la portata dello schema di idealizzazione. Anzitutto, introduciamo la *fbf* $\phi(x; y) = x \in b \wedge y \neq x$.

Proposizione 5.3.6. *Tutti gli elementi degli insiemi finiti standard sono standard.*

Dimostrazione. Applichiamo I con ϕ a un insieme finito standard b. Se $a = b$ non esiste alcun $x \in b$ che soddisfi la *fbf* per ogni $y \in b$. Dunque la $i)$ è falsa e quindi non esiste alcun x tale che sia $\forall^{st} y(x \in b \wedge y \neq x)$,, quindi in b non vi è alcun x non standard, da cui l'enunciato. □

Corollario 5.3.7. *Ogni sottoinsieme di un insieme finito e standard è standard.*

Dimostrazione. Se a è finito e standard e b è un sottoinsieme di a, allora $\{x \in a;\ x \in b\}^{st} = b$. $\square$

Proposizione 5.3.8. *Ogni insieme infinito contiene elementi non standard.*

Dimostrazione. Esaminiamo adesso la stessa fbf ϕ della proposizione precedente, ma con b insieme infinito: allora la $i)$ vale e quindi l'implicazione verso $ii)$ di I assicura che esiste un elemento x di b non standard. $\square$
Si noti che non è richiesto alle altre variabili di $\phi(x; y)$ di essere necessariamente standard: I si applica anche se b in ϕ non lo è.

Se si applica I alla stessa fbf della proposizione 5.3.6, ma con b non standard, segue che

Proposizione 5.3.9. *Ogni insieme non standard ha elementi non standard.*

Dimostrazione. Infatti, dato un qualsiasi insieme finito standard a e uno non standard b, per il corollario 5.3.7 esiste un $x \in b$ non appartenente ad a, altrimenti risulterebbe $b \subseteq a$ e b standard. Quindi x è diverso da tutti gli $y \in a$. Esiste allora per I un $x \in b$ diverso da tutti gli y standard. $\square$
Dai risultati precedenti segue subito

Corollario 5.3.10. *Un insieme ha tutti gli elementi standard se e solo se è finito e standard.*

Una conseguenza piuttosto strana di I è la seguente.

Proposizione 5.3.11. *Tutti gli insiemi standard sono elementi di un insieme finito U, ovviamente non standard.*

Dimostrazione. Si usi ancora l'implicazione $i) \Rightarrow ii)$ in I con la fbf $Fin(x) \wedge y \in x$: la $i)$ stavolta risulta verificata (basta prendere $x = a$) e quindi vale la $ii)$. Dunque esiste un insieme x finito che contiene tutti gli insiemi standard y. $\square$

Osservazioni 5.3.12.

- L'insieme U ottenuto è un analogo della classe universale $\mathbf{U}$ (osservazioni 2.0.4): si evita il paradosso perché esso contiene soltanto tutti gli insiemi *standard*.
- Dato un insieme b qualunque, l'intersezione $b \cap U$ è un sottoinsieme finito di b che ha tra i suoi elementi tutti i suoi elementi standard.
- Modificando la fbf impiegata in $Fin(x) \wedge y \in x \wedge \psi(x)$ si può ottenere un 'insieme universale' che condivida qualunque proprietà ψ di cui godano tutti gli insiemi finiti standard.

Vediamo ora un esempio importante.

Esempio 5.3.13. L'insieme $\mathbb{N}$ dei numeri naturali è un insieme classico, ma essendo infinito, ha elementi non standard. Dal momento che i numeri naturali standard sono insiemi finiti, i naturali non standard devono essere infiniti rispetto alla relazione d'ordine classica, che coincide con $\in$. In effetti, applicando I alla fbf

$$x \in \mathbb{N} \wedge y \in \mathbb{N} \wedge y < x$$

si ha: esiste $x_0 \in \mathbb{N}$ maggiore di ogni $n \in \mathbb{N}$ standard: ovviamente x_0 *non* è standard! È questo il senso in cui I postula l'esistenza di elementi 'ideali', in analogia con idee classiche della matematica, come punti 'all'infinito', o simili: gli elementi *non* standard si possono pensare come elementi 'infiniti', non descrivibili in concreto. C'è analogia con certi modelli dell'aritmetica di Peano, per cui vedi *Appunti sulla ricorsività*, 4.4.

Consideriamo ora una significativa applicazione dello schema S.

Esempio 5.3.14. Sebbene da un insieme e e da un predicato classico (interno) si possa sempre ottenere per specificazione un sottoinsieme, da una proprietà non classica ψ e da un insieme e non si ottiene mediante S l'insieme di tutti e soli gli $x \in e$ per cui vale ψ: ad esempio, per unicità

$$\{x \in \mathbb{N}; St(x)\}^{st} = \mathbb{N}, \quad \emptyset = \{x \in \mathbb{N};\ \neg St(x)\}^{st}$$

e non esiste l'insieme di tutti e soli i numeri naturali non standard ('infiniti'): se ci fosse, avrebbe minimo k, (proprietà classica), che sarebbe 'infinito' e $k-1$ sarebbe ancora un suo elemento. Si confronti la situazione con quella che si ha col segno $<<$ ('trascurabile'): i numeri 'infiniti' sono quelli rispetto ai quali gli altri sono trascurabili, ma non ha senso parlare del più piccolo numero di questo tipo.

In altri termini, IST evita i paradossi escludendo non soltanto le collezioni troppo grandi, ma anche quelle vaghe, sicché si ha una idea di insieme profondamente diversa da quella usuale: gli insiemi sono collezioni non troppo grandi ma anche non troppo irregolari.

5.3.3 L'analisi non standard

La IST si è sviluppata dall'Analisi non standard di A. Robinson, che negli anni intorno al 1960 riuscì a giustificare in termini logicamente ineccepibili l'uso euristico tradizionale di infinitesimi ed infiniti in Analisi, bandito (almeno a parole) dalla fine dell'Ottocento per la rigorizzazione dei fondamenti operata da Cauchy a Weierstraß (e Cantor).

Nell'Analisi non standard l'approccio è tuttavia di tipo prevalentemente semantico: si introduce un modello $\mathbb{R}^*$ della teoria elementare dei numeri reali diverso da $\mathbb{R}$ ma ad esso elementarmente equivalente: quello dei numeri *iperreali*. In esso quindi hanno le consuete proprietà le operazioni e le disuguaglianze, descritte dagli assiomi di campo ordinato [5] , e quindi il valor assoluto, eccetera. Invece entro IST si tratta soltanto dei numeri reali, ma tra essi compaiono, anche a livello di teoria, numeri reali non standard, elementi dell'insieme (standard, ma infinito) indicato sempre con $\mathbb{R}$. In entrambi gli approcci, è centrale il ruolo di numeri reali infinitesimi, infiniti, limitati. Esponiamo queste definizioni con i simboli di IST.

[5] Per quanto riguarda l'assioma dell'estremo superiore, va formulato come schema usando fbf, non essendo possibile quantificare su sottoinsiemi di $\mathbb{R}$.

Definizioni 5.3.15.

- $x \in \mathbb{R}$ è *limitato* se esiste un y reale standard positivo tale che $|x| < y$;
- $x \in \mathbb{R}$ è *infinito* se per ogni y reale standard positivo $|x| > y$;
- $x \in \mathbb{R}$ è *infinitesimo* se per ogni y reale standard positivo $|x| < y$;
- Due numeri reali x, y sono *infinitamente vicini* ($x \approx y$) se $|x - y|$ è infinitesimo;
- Se $x \in \mathbb{R}$ è limitato, esiste sempre uno y reale standard (unico) tale che $x \approx y$: esso è la *parte standard di x*, ed è indicato con $st(x)$ o x^*.

Osservazione 5.3.16. L'esistenza di tali numeri non standard si può provare in maniera simile a quella esposta per trovare numeri naturali non standard (esempio 5.3.13): si prova l'esistenza di numeri (non standard) maggiori di ogni numero reale standard; poi, per passaggio al reciproco e all'opposto, di numeri infinitesimi positivi e negativi; e così via.

Si possono così esporre in maniera rigorosa e al tempo stesso intuitiva molte dimostrazioni classiche dell'Analisi. A questo proposito, esiste ormai una tradizione didattica, specie negli Stati Uniti: un manuale elementare molto fortunato è stato [Keisler 1976], tradotto anche in italiano (Ed. Piccin, Padova).

IST si può pensare come la teoria degli insiemi collegata all'Analisi non standard, come ZF è sorta dall'Analisi classica. I concetti fondamentali della seconda si possono definire in IST per spazi metrici e topologici: ad esempio, $x \approx y$ in uno spazio metrico standard $(M; d)$ significa che $d(x, y) \approx 0$; se $A \subseteq M$,

$$A^* = \{x \in M;\ \exists y \in A, x \approx y\}^{st}$$

si chiama l'*ombra* di A. A^* è sempre chiuso; se A è standard, A^* è dunque $\overline{A}$, cioè la sua chiusura. Si può così riformulare molta topologia elementare in termini più vicini all'intuizione geometrica. I risultati fondamentali per spazi metrici (od anche topologici) rimangono validi in generale, dato che le definizioni di aperto, chiuso, compatto sono classiche. Le dimostrazioni sono però spesso più semplici. Non mancano tuttavia difficoltà, almeno per mancanza di abitudine ai nuovi assiomi: ad esempio, per evitare contraddizioni, non si può ammettere che l'applicazione $x \mapsto x^*$ (definita, diciamo, per gli $x \in \mathbb{R}$ limitati) sia una funzione: il suo grafico (e, del resto, il suo dominio) non sono insiemi in IST.

Un'altra notevole applicazione di IST consiste nella esposizione non standard della probabilità finita.

5.4 Teorie 'stratificate': NFU

Una presentazione della teoria degli insiemi assai diversa è quella che deriva dalla *teoria dei tipi* di Russell, tramite il sistema NF ('New Foundations') di W. v.O. Quine, modificato da B. Jensen in NFU ('**N**ew **F**oundations with **U**relementen'). Questa impostazione parte dall'idea di complessità di un insieme, che viene pensato come una entità a più livelli: da oggetti si passa a insiemi, poi a insiemi di insiemi,... Se $x \in y$, y dovrebbe dunque avere un livello, un *tipo*, superiore rispetto ai suoi elementi x, espresso mediante un intero maggiore di una unità rispetto a quello degli x. Di qui il termine *stratificazione* (dei tipi). Consideriamo brevemente questo approccio, seguendo la presentazione di [Holmes 1998], senza alcuna pretesa di completezza —e senza riportare dimostrazioni, al solo scopo di illustrare una idea di insieme profondamente diversa da tutte le altre: ulteriore prova della complessità di questa nozione, in apparenza così poco problematica.

5.4.1 Idee fondamentali

In questa teoria non compaiono soltanto insiemi, ma 'oggetti' più generali che possono non esserlo (detti allora *atomi*, gli *Urelementen* della sigla), ma che comunque possono appartenere come elementi a insiemi: per semplificare la trattazione, usiamo lettere maiuscole ($A, B, \ldots$) per insiemi e lettere minuscole $(x, y, \ldots)$ per oggetti qualunque. Tra gli oggetti vanno incluse le coppie ordinate $(a; b)$ esistenti per tutti gli oggetti a, b: per ragioni di semplicità non viene usata, anche se sarebbe possibile, la classica definizione di Kuratowski 2.2.2. Sempre per maggior semplicità oltre al predicato di uguaglianza $=$ e a quello di appartenenza $\in$, si introducono le due *proiezioni* π_1 e π_2: $x\pi_1 y$ sussiste se x è una coppia ordinata di prima componente y e analogamente per π_2.

L'assioma di estensione vale naturalmente solo per insiemi:

Assioma di estensione per NFU [E]
Dati *insiemi* X e Y, se essi hanno gli stessi elementi, allora sono uguali: $X = Y$

Per lo sviluppo della teoria di base si introducono altri due assiomi:

Assioma degli atomi per NFU [A]	**Assioma delle coppie per NFU [C]**
Nessun atomo ha elementi	Per ogni x e per ogni y esiste $(x; y)$ e $(a; b) = (c; d)$ se e solo se $a = c$ e $b = d$

Come sempre però il punto cruciale consiste nel limitare il principio di comprensione. Definiamo anzitutto cosa si debba intendere per *fbf stratificata*:

Definizione 5.4.1. Una fbf ϕ con simboli propri $=$, $\in$, π_1, π_2 è stratificata se ad ogni occorrenza di una sua variabile si può assegnare un ben preciso intero (il *tipo* della variabile) in modo tale che

- nelle fbf atomiche $x = y$, $x\pi_1 y$ e $x\pi_2 y$ di ϕ, sia x che y hanno lo stesso tipo;
- in $x \in y$, x ha tipo inferiore di una unità rispetto a y.

Osservazioni 5.4.2.
- La idea alla base della definizione è che un insieme ha 'tipo di stratificazione' superiore —di una unità— rispetto ai suoi elementi. Per semplificare è preferibile allora non utilizzare coppie

‘alla Kuratowski’ che lo innalzerebbero di due unità, ma introdurre le proiezioni, che danno coppie con lo stesso tipo delle componenti: una coppia $w = (x; y)$ ha tipo uguale a quello di x, y, dato il modo in cui viene definita la stratificazione, e visto che $w\pi_1 x$ e $w\pi_2 y$.

- Le costanti e in genere i simboli introdotti nella teoria successivamente vanno rimpiazzati dalle opportune *fbf* definitorie, secondo la relativa teoria *delle descrizioni*, risalente anch’essa a Russell; più esplicitamente, nel caso di costanti,

- se $\phi(x)$ è stratificata e c è una costante definita da una *fbf* stratificata ψ, $\phi[x|c]$ [6] risulta ancora stratificata, eventualmente aumentando di un opportuno numero intero i tipi delle variabili coinvolte, cosa sempre possibile.

Si introduce allora lo schema di comprensione opportuno:

Schema di comprensione stratificata per NFU [CS]
Se ϕ è stratificata, esiste l’insieme $\{x; \phi\}$

La importanza di questo schema è notevolissima. Vediamo alcune conseguenze e osservazioni al proposito.

Osservazioni 5.4.3.

- Siccome ad esempio $x = x$ è stratificata, l’universo $U = \{x; x = x\}$ è un insieme, come indica il titolo di [Holmes 1998]!

- Gli atomi non hanno elementi, ma vi è anche un *insieme* senza elementi, $\emptyset$ (nel testo citato, $\{\}$), dato che $x \neq x$ è ugualmente stratificata.

- Più in generale, se A è un insieme, è stratificata $x \notin A$ e quindi è un insieme $A^c = \{x;\ x \notin A\}$, il *complementare* di A, che in ZF non è *mai* un insieme. Dato che unione e intersezione di insiemi sono ugualmente definibili con formule stratificate, l’universo insiemistico ha una struttura elementare di algebra di Boole.

[6] $\phi[x|c]$ è il risultato della sostituzione di tutte le occorrenze libere di x in ϕ con c.

- Sono poi relazioni a pieno titolo, in quanto insiemi (in questo senso) di coppie ordinate, l'inclusione (si verifichi che è stratificata $\forall x\,(x \in A \Rightarrow x \in B)$), le proiezioni: sono per esempio insiemi in NFU

$$\pi_1 = \{z;\ \exists x\,\exists y\, z = ((x;y);x)\} \tag{5.1}$$

  l'uguaglianza tra oggetti, l'equipotenza tra insiemi A e B, eccetera.

- Si dice che i simboli predicativi $=$, π_1, π_2 sono *realizzati* nella teoria; se è necessario distinguere il simbolo dall'insieme si usano parentesi quadre, così l'insieme 5.1 è più esattamente indicato con $[\pi_1]$. Questa distinzione naturalmente fa capire che non tutti i predicati sono realizzabili in NFU; infatti non lo è il predicato fondamentale $\in$.

- Perché $[\pi_1]$ è un insieme? Perché può venir descritto da una formula stratificata:

$$[\pi_1] = \{((x;y);x);\ x,y \in U\} = \{z;\ \exists w\,\exists x\,\exists y(z\pi_1 w \wedge z\pi_2 x \wedge w\pi_1 x \wedge w\pi_2 y)\}$$

  Le coppie ordinate hanno infatti lo stesso tipo delle componenti. Per lo stesso motivo $domR = \{x; \exists y\,(x;y) \in R\}$, il *dominio* di una relazione R, è sempre un insieme (provarlo per esercizio).

- Molti di questi insiemi ($[=]$ eccetera) sono introdotti in [Holmes 1998] con appositi assiomi, casi particolari dello schema citato, che viene provato come teorema sulla base di alcuni di essi: una presentazione analoga a quella vista in NBG (sezione 5.2), sempre per specificare la portata e i limiti nella teoria del principio di comprensione. Questa presentazione degli assiomi ha il vantaggio di mostrare come la teoria possa —almeno fino a questo punto— essere finitamente assiomatizzata.

- Se B è un insieme si può comunque definire l'insieme potenza: $A \subseteq B$, come si è visto, è stratificata —A e B possono avere lo stesso tipo— e $\mathcal{P}\{B\}$ è perciò un insieme: avrà tipo superiore di uno rispetto ad A nel definire altri insiemi. Non risulta in una contraddizione il fatto che

$\mathcal{P}\{U\} \subseteq U$: comprensibilmente, poiché U ha per elementi anche atomi (vedi il teorema di Specker 5.4.14).

- La formula precedente però non è stratificata, così come non lo è ad esempio la definizione del successore di un insieme $A \cup \{A\}$. I singoli insiemi successori però esistono come 'casi particolari' di $A \cup \{B\}$, dato che la sostituzione è ammessa nei parametri delle formule definitorie, ma non è possibile usarli per formare altri insiemi mediante CS. Quindi insiemi definiti da formule *non* stratificate possono 'esistere', cioè essere considerati insiemi nella teoria, a meno che non portino a contraddizione. Non si possono però utilizzare in dimostrazioni generali, dove, parlando approssimativamente, si possono sfruttare soltanto formule stratificate.

- Il paradosso di Russell viene trattato classicamente: $x \notin x$ non è stratificata e si prova appunto che, portando all'usuale contraddizione, la collezione relativa non può far parte, come insieme, dell'universo descritto dalla teoria — è quella che nella terminologia adottata da [Holmes 1998] viene chiamata una classe propria.
  Più esattamente, si prova per assurdo che $[\in]$ non è un insieme, cioè $\in$ non è realizzata: infatti allora sarebbe un insieme $R = \{x;\ x \notin x\} =$ $= dom([=] \cap [\in]^c)$ e si produrrebbe la solita contraddizione
  $$R \in R \Leftrightarrow R \notin R.$$

- Spesso bisogna ricorrere, per non violare la stratificazione, ai singoletti $\{x\}$ —che sono insiemi, qualunque oggetto x contengano, e sono facilmente definibili, nonché al loro insieme totale $\mathcal{P}_1\{U\}$, o a quello relativo a un insieme A: $\mathcal{P}_1\{A\}$. In questi casi, le parentesi graffe segnalano appunto un 'passaggio ai singoletti' che innalza il tipo di uno.

- Per le relazioni R è importante considerare la sua *immagine con singoletti*
  $$SI\{R\} = \{(\{x\};\{y\});\ (x;y) \in R\}.$$

In sé l’operazione di formare il singoletto, $x \mapsto \{x\}$, si dimostra essere una classe propria —la sua definizione non è del resto stratificata.

Definizioni 5.4.4.

- Un insieme è cantoriano se $A \sim \mathcal{P}_1\{A\}$, nel senso che esiste una corrispondenza biunivoca (un certo insieme di coppie della teoria) tra A e $\mathcal{P}_1\{A\}$;
- se $x \in A \mapsto \{x\} \in \mathcal{P}_1\{A\}$ è una funzione di dominio A, essa è una corrispondenza biunivoca: si dice allora che A è fortemente cantoriano.

5.4.2 I numeri naturali; cardinali e ordinali

Dallo schema di comprensione stratificata si possono derivare le costruzioni fondamentali in ZF, —unione, coppia, potenza, e anche lo schema di rimpiazzamento per fbf stratificate opportunamente; naturalmente con riferimento a questo tipo di ‘insiemi’. Si può derivare anche l’assioma dell’infinito.

Come in ZF, ma in maniera ancor più significativa, occorre l’assioma di scelta e non solo per sviluppare la teoria dei numeri cardinali; ma esso va ora formulato in maniera non funzionale, come assioma di selezione (vedi teorema 3.2.4), dato che $f(C) \in C$ non è stratificata:

Assioma di scelta per NFU [AS]
Se A è un insieme non vuoto di insiemi non vuoti e a due a due disgiunti, esiste un insieme B (*di selezione* per A) tale che $\forall C \in A\, \exists x\; B \cap C = \{x\}$

CS però comporta anche notevoli limitazioni. Questo ha profondi riflessi sulla teoria classica dei numeri cardinali e ordinali, a partire dai numeri naturali: gli ordinali di von Neumann, pur esistenti come singoli insiemi in NFU, sono dati da formule non stratificate e non costituiscono un insieme (una forma del paradosso di Burali-Forti).

I numeri naturali in NFU

I numeri naturali si possono introdurre ‘alla Frege’ come insiemi di insiemi ‘finiti’ equipotenti. Anzitutto, $0 = \{\emptyset\}$, $1 = \mathcal{P}_1\{U\}$ —gli insiemi degli insiemi con zero oppure esattamente un unico elemento. Si usa poi una operazione di successore stratificata per introdurre gli altri numeri naturali n come classi di equivalenza di insiemi finiti: per insiemi A, B si vuole ottenere, come per tutti i numeri cardinali

$$(A \in n \wedge B \in n) \Rightarrow B \sim A \text{ e viceversa } (A \in n \wedge B \sim A) \Rightarrow B \in n.$$

Esponiamo le principali definizioni, tralasciando le dimostrazioni, anche quelle che giustificano la correttezza delle definizioni stesse.

Definizioni 5.4.5.

- Dato un insieme di insiemi A, il successore di A è l'insieme $S(A) = \{a \cup \{x\};\ a \in A \wedge x \notin a\}$, e
- la corrispondenza $A \mapsto S(A)$ è una funzione S, nel solito senso di insieme univoco di coppie.
- Si definisce la induttività per questi insiemi nel solito modo: $IND(X)$ abbrevia $0 \in X \wedge (A \in X \Rightarrow S(A) \in X)$;
- $\mathcal{N}$, l'intersezione di tutti gli insiemi induttivi è il minimo insieme induttivo possibile: i suoi elementi sono i numeri naturali di NFU.
- L'unione $\bigcup \mathcal{N}$ è l'insieme Fin degli insiemi finiti di NFU, essendo costituita da elementi di elementi di $\mathcal{N}$, cioè da elementi dei numeri naturali.

È notevole il fatto che non si debba ricorrere a un assioma dell'infinito per giustificare l'esistenza dell'insieme dei numeri naturali $\mathcal{N}$ e gli assiomi, poi le regole dell'aritmetica di Peano. Tuttavia, perché $\mathcal{N}$ sia un ragionevole insieme di numeri naturali, bisogna provare che per ogni $A \in n$, cioè per ogni A finito, $S(A)$ contiene insiemi ‘con un elemento x in più’ rispetto agli $a \in A$. Se non fosse possibile scegliere sempre $x \notin a$, $S(A) = \emptyset$: perciò l'assioma dell'infinito diventa curiosamente il teorema

$$\emptyset \textit{ non è un numero naturale}$$

Tuttavia non è possibile provare in generale che $A \in n \Leftrightarrow \mathcal{P}_1\{A\} \in n$ (solo caso per caso, sempre per mancanza di stratificazione), sicché si deve introdurre un n ‘di tipo superiore’, che è ben definito:

Definizione 5.4.6. $T\{n\}$ è il numero naturale che contiene come elementi tutti i $\mathcal{P}_1\{A\}$ con $A \in n$.

$T\{n\}$ è di tipo superiore di uno rispetto a n: per evitare questa moltiplicazione di tipi di naturali, già Russell introdusse

Assioma del contare per NFU [AC]
$T\{n\} = n.$

Segue che alle variabili ristrette ai naturali si può attribuire qualunque tipo.

I numeri ordinali in NFU

Per gli ordinali la relazione rilevante è naturalmente la similarità tra buoni ordinamenti. Gli ordinali vengono definiti, in maniera essenzialmente analoga ai numeri naturali, come *insiemi* (classi di equivalenza) di buoni ordinamenti simili.

Definizioni 5.4.7.

- L’insieme (classe di equivalenza) dei buoni ordinamenti simili a un buon ordinamento S è un ordinale, e si dice tipo d’ordine di S.
- L’insieme degli ordinali si indica con ORD.

Osservazioni 5.4.8.

- Le definizioni sono corrette perché sono stratificate. Però si riferiscono direttamente alle relazioni di buon ordine e non agli insiemi bene ordinati da esse (il loro dominio).
- I numeri naturali *non* sono ordinali, anche se i buoni ordinamenti degli insiemi finiti danno luogo a ‘numeri naturali ordinali’ $0, 1, 2, \ldots$

Si può definire una relazione di buon ordine tra ordinali α, β per mezzo di buoni ordinamenti $R \in \alpha$, $S \in \beta$.

Definizione 5.4.9. Se $S \in \beta$ è una continuazione [7] di un ordinamento simile a $R \in \alpha$, allora $\alpha < \beta$.

Il relativo tipo d'ordine di ORD si indica con Ω. Tuttavia, questo non porta a contraddizione. Come si evita il paradosso di Burali-Forti? Si può osservare che nella usuale teoria,
il tipo d'ordine dell'insieme dei segmenti iniziali propri di un ordinale α fissato, rispetto all'inclusione, ridà α stesso (teorema 4.2.3):
questo anzi è banalmente implicito nella definizione di von Neumann degli ordinali. Se a questo insieme si aggiunge α si ottiene $S(\alpha)$, un ordinale strettamente maggiore, il che, applicato alla collezione di tutti gli ordinali, bene ordinata nel modo naturale, dà il paradosso.

In NFU Ω e un ordinale qualsiasi α hanno tipi di stratificazione differenti: il primo ha un tipo superiore di due unità, perché tra i suoi elementi compare la relazione d'ordine tra ordinali, che è un insieme di coppie di ordinali.

Seguendo l'impostazione precedente,un confronto si può allora soltanto istituire tra:

(a) l'ordinale, ben definito, $T^2\{\alpha\}$ [8] dei segmenti iniziali di buoni ordinamenti $S \in \alpha$, con l'ordine naturale;

(b) Ω stesso.

Si può allora provare che $T^2\{\alpha\}$ è minore di Ω: nel caso di Ω si ottiene allora non il paradosso, ma per assurdo che $T^2\{\Omega\}$ è *strettamente minore* di Ω stesso, e questo evita la contraddizione, se non la stranezza, del paradosso di Burali-Forti.

Se alle relazioni $S \in \alpha$ si sostituiscono le immagini con singoletti $SI\{R\}$ si ottiene un ordinale 'di tipo superiore' $T\{\alpha\}$: nella discussione precedente, $T^2\{\alpha\}$ indica la costruzione SI applicata due volte, equivalente a quella citata. Gli ordinali *cantoriani* sono definiti da

[7] Per esercizio, determinare l'esatta definizione di questa proprietà, che è semplicemente l'inverso della nozione di segmento iniziale, applicata agli ordinamenti.

[8] L'esponente 2 indica l'elevamento del tipo di stratificazione di due unità.

Definizioni 5.4.10.
- α è cantoriano se $T\{\alpha\} = \alpha$ o equivalentemente $S \in \alpha$ è un ordinamento cantoriano, o ancora $domS$ è cantoriano;
- α poi è fortemente cantoriano se contiene ordinamenti $S \in \alpha$ fortemente cantoriani, o ancora se $domS$ è fortemente cantoriano.

La terminologia non è del tutto coerente con quella per insiemi qualunque, ma l'analogia rimane, come si vede, stretta. Il riferimento è naturalmente alla definizione di ‘cantoriano’ o ‘fortemente cantoriano’ per insiemi generici: definizioni 5.4.4. Comunque ‘fortemente cantoriano’ implica ‘cantoriano’.

Per gli ordinali cantoriani il paradosso ha la stessa conclusione che nel caso classico: essi non costituiscono un insieme, ma solo una classe propria. Questo ha una certa analogia con quello che si verifica in IST: sottocollezioni di insiemi, in questo caso di ORD, possono non essere insiemi.

La teoria dei numeri ordinali e specialmente i legami tra NFU e ZFC possono essere chiariti e semplificati da assiomi aggiuntivi, ad esempio lo *schema dei piccoli ordinali* per cui si rimanda specificamente a [Holmes 1998, 15.3]. Una sua immediata conseguenza è l'assioma del contare AC.

I numeri cardinali in NFU

Gli stessi problemi di stratificazione si presentano per i cardinali come per gli ordinali: però questo impedisce il prodursi del paradosso di Cantor.

La definizione di numero cardinale è intuibile:

Definizione 5.4.11. Un numero cardinale è una classe di equivalenza rispetto alla relazione di equipotenza tra insiemi. La cardinalità (numero cardinale) $|A|$ di un insieme A è l'insieme $\{B;\ B \sim A\}$.

I numeri naturali sono particolari cardinali, mentre differiscono (ma si possono identificare) con i corrispondenti ordinali.

La teoria si può sviluppare in maniera molto simile a quella di ZFC, ma, per la presenza di atomi, come vedremo inevitabile, il teorema di Cantor può venir dimostrato per insiemi A soltanto usando $\mathcal{P}_1\{A\}$.

Teorema 5.4.12. ***(Cantor)*** *Per ogni insieme A,* $|\mathcal{P}_1\{A\}| < |\mathcal{P}\{A\}|$.

e quindi si ottiene soltanto un paradossale ma non contraddittorio

Corollario 5.4.13.

$$|\mathcal{P}_1\{U\}| = |1| < |\mathcal{P}\{U\}| \leq |U|$$

giacché non è possibile mettere in corrispondenza biunivoca U e $\mathcal{P}_1\{U\}$ con la corrispondenza 'naturale' $x \mapsto \{x\}$, inesistente come insieme di NFU. In questo modo viene evitato il paradosso di Cantor.

Addirittura, si dimostra

Teorema 5.4.14. ***(Specker)*** $|\mathcal{P}\{U\}| < |U|$*, e quindi devono esistere atomi.*

Questo teorema, per cui sembra inevitabile il ricorso all'assioma di scelta, prova esplicitamente che *devono esistere atomi*: sebbene molti risultati precedenti si possano spiegare intuitivamente con la loro esistenza, questo è l'unico risultato positivo in tal senso.

Anche in questo caso, la teoria si avvicina a quella 'classica' nel caso di cardinali cantoriani:

Definizioni 5.4.15.

- Un cardinale $|A|$ è cantoriano se lo è A;
- un cardinale $|A|$ è fortemente cantoriano se lo è A.

Valgono le osservazioni fatte nel caso delle analoghe definizioni per ordinali.

Per gli insiemi cantoriani A vale il teorema di Cantor nella forma consueta per i relativi cardinali: $|A| = |\mathcal{P}_1\{A\}| < |\mathcal{P}\{A\}|$.

Relazioni tra NFU e ZFC

ZFC può essere interpretata come una sottoteoria di NFU, ma vale anche il viceversa. Anzitutto, la consistenza di NFU può essere accertata su basi più deboli che non quella di ZF; tuttavia in ZFC stessa si può costruire un modello (cioè definire una classe di insiemi) in cui vale NFU, usando la *gerarchia cumulativa degli insiemi* (pagina 82).

Inversamente si ha, ammettendo l'assioma dei piccoli ordinali:

Proposizione 5.4.16. *Tutti gli insiemi (quindi gli ordinali, o i cardinali) cantoriani sono fortemente cantoriani.*

Su questa base, si può costruire un modello di ZFC usando gli ordinali cantoriani.

Teorema 5.4.17. *ZFC ha per modello in NFU, con opportuna interpretazione, la classe degli ordinali cantoriani.*

Infine, anche l'analisi non standard può essere interpretata come una parte di NFU concernente i numeri reali.

Appendice A

Richiami di aritmetica e algebra

A.1 Alcuni simboli

Anzitutto, simboli per i più consueti insiemi numerici e le funzioni caratteristiche.

- Per gli insiemi numerici, usiamo i consueti caratteri 'da lavagna': $\mathbb{N}$ l'insieme dei naturali, zero incluso ($\mathbb{N}^+$ indica i naturali diversi da zero); $\mathbb{R}$ l'insieme dei reali, e così via.
- Per gli intervalli di $\mathbb{R}$ si usa la consueta notazione con parentesi quadre.
- Le funzioni caratteristiche di un sottoinsieme A di X vengono indicate con χ_A, sottointendendo il dominio X: esse assumono il valore 1 in corrispondenza degli elementi di A e valgono zero altrove.

Anche col rischio di introdurre convenzioni non usuali, se ne sono usate alcune per gli indici numerici, che riportiamo da *Appunti sulla ricorsività*:

A.1.
- con h, k, n, r si indicheranno indici che possono assumere valori in $\mathbb{N}$ *diversi da zero*;
- con i, j, l, m si indicheranno invece indici che possono assumere valori in $\mathbb{N}$ *anche uguali a zero*;

- con $x, y, z, u, \ldots$ si indicheranno variabili generiche: la distinzione tra indici e variabili è naturalmente di comodo;
- con ${}^m x = (x_1, \ldots, x_m)$ si indicherà una m-upla di variabili (o *parametri*), eventualmente mancanti (può essere $m = 0$);
- analogamente per ${}^n x = (x_1, \ldots, x_n)$ (ma qui i parametri saranno almeno uno) e simili;
- per mettere in evidenza una variabile, non necessariamente l'ultima, in una $(n+1)$-upla si scriverà $({}^n x, y)$ o $({}^n x, z)$ o simili.
- Convenzioni analoghe alle ultime per m-uple di variabili quantificate, come nella logica del primo ordine. Ad esempio, $\exists^k x \in \mathbb{N}^k$ sta per $\exists x_1 \in \mathbb{N} \ldots \exists x_k \in \mathbb{N}$.
- In teoria degli insiemi si fa largo uso di *quantificazioni limitate* a un insieme, come sopra, o ad un predicato M (una classe, indicata in grassetto, $\mathbf{M}$): $\forall x \in \mathbf{M}\phi$ vale $\forall x M(x) \Rightarrow \phi$, eccetera, come viene ricordato nel testo.

A.2 Aritmetica: Sistemi di numerazione

Ricordiamo, senza dimostrazioni o riferimenti, l'aritmetica elementare della consueta rappresentazione posizionale dei numeri.

Un sistema di numerazione (posizionale, a base costante) è costituito da un numero naturale $b \geq 2$ (la *base*) e dall'insieme delle sue *cifre* $D = D_b = \{0, \ldots, b-1\}$. Identifichiamo le cifre coi loro simboli usuali. Nei casi in cui $b > 10$ però diviene necessario introdurre nuovi simboli per le cifre maggiori di 9.

Definizione A.2.1. Sia $x \in \mathbb{N}$: se $x = \sum_{j=0}^{m} d_j b^j$, $d_j \in D_b$, $d_m \neq 0$ se $m \neq 0$, si dice che $x = (d_m \ldots d_0)_b$ (o semplicemente $x = d_m \ldots d_0$) è una rappresentazione di x in base b.

Esempi A.2.2.

- Tra le cifre compaiono sempre 0 e 1: quindi zero si rappresenta sempre ovviamente con '0', e uno con '1'.

- Se x è ventitré, si ha $x = (23)_{dieci} = (10111)_{due} = (212)_{tre}$, poiché $x = 2 \cdot 10 + 3 = 2^4 + 2^2 + 2 + 1 = 2 \cdot 3^2 + 3 + 2$. Nelle somme precedenti viene impiegata la rappresentazione decimale per chiarezza; si noti che la base ('dieci' di solito viene omessa) è scritta in italiano, per evitare confusione: la base b verrebbe sempre rappresentata con '10'!

Teorema A.2.3. *Ogni $x \in \mathbb{N}$ ha esattamente una rappresentazione in base b, qualunque sia $b \geq 2$.*

Passiamo ora a considerare la rappresentazione in base b (o b-esimale) di un numero reale x: dato che i numeri negativi si possono rappresentare come opposti dei positivi con l'uso del segno meno e che un numero $y \geq 0$ si può scomporre nella somma di un numero naturale n più un numero $x \in [0;1]$, ci si può limitare a quest'ultimo caso (teorema seguente).

Definizioni A.2.4.

- Una successione di cifre b-esimali $(c_n)_{n=1}^{\infty}$ si dice un *allineamento b-esimale*;

- in corrispondenza di questo allineamento si ha uno *sviluppo b-esimale*, che è la serie a termini non negativi $\sum_{n=1}^{\infty} \frac{c_n}{b^n}$.

Si prova ora facilmente il seguente teorema:

Teorema A.2.5.

- *Ogni allineamento b-esimale $(c_n)_{n=1}^{\infty}$ dà luogo a uno sviluppo convergente a un $x \in [0;1]$; si scrive allora $x = (0, c_1 c_2 c_3 \ldots)_b$ e si dice che questo sviluppo è una rappresentazione b-esimale di x;*

- $0 = 0,000\ldots$ *e rispettivamente* $1 = 0,(b-1)(b-1)(b-1)\ldots$ *sono le uniche rappresentazioni di 0 e 1;*

- *viceversa, ogni $x \in [0;1]$ ha (almeno) una rappresentazione b-esimale.*

La questione dell'unicità della rappresentazione è più complessa. Anzitutto, qualche definizione.

Definizioni A.2.6. • Un allineamento b-esimale $(c_n)_{n=1}^{\infty}$ (o il relativo sviluppo, o rappresentazione) si dice *periodico* se da un certo momento in poi una stringa di cifre (il *periodo*) si ripete indefinitamente. Un periodo viene rappresentato con una sopralineatura;

- se il periodo è 0, si parla di allineamento (o sviluppo, o rappresentazione) *finito*, e il periodo non viene scritto nello sviluppo (rappresentazione): i numeri con questi sviluppi sono i numeri *b-esimali finiti*. Se il periodo è $(b-1)$ si parla di allineamento (sviluppo) *improprio*;

- nell'ultimo caso si parla di rappresentazione impropria, mentre le altre rappresentazioni (o allineamenti, o sviluppi) si dicono *proprie*.

Esercizi A.2.7. • Provare che $\frac{4}{33} = 0,\overline{12} = 0,1\overline{21}$, $b = dieci$ (ma la rappresentazione è unica!)

- Provare che $\frac{1}{5} = 0,1\overline{9} = 0,2$ ($b = dieci$)

- Provare che $\frac{2}{9} = (0,\overline{2})_{dieci} = (0,02)_{tre}$

Si ha anzitutto

Teorema A.2.8. *In ogni base, i numeri che hanno sviluppi periodici sono tutti e soli i razionali.*

Si può soprattutto enunciare un teorema di unicità:

Teorema A.2.9. *Sia $0 < x < 1$. x ha una unica rappresentazione b-esimale, a meno che non sia b-esimale finito: in tal caso, ha esattamente un'altra rappresentazione, che è impropria.*

Se infine $y \geq 0$, $y = n + x$ con $n \in \mathbb{N}$, $x \in [0;1]$ rappresentati in base b con $n = (d_m \ldots d_0)_b$ e $x = (0,c_1c_2c_3\ldots)_b$ una rappresentazione di y è $y = (d_m \ldots d_0, c_1c_2c_3\ldots)_b$. Il teorema precedente vale allora per ogni $y > 0$ e, posto $d_{-n} = c_n$, si ha un corrispondente sviluppo di y: $y = \sum_{j=-\infty}^{m} d_j b^j$. L'unicità viene a mancare sia per la possibilità di più decomposizioni in somma tra un naturale e un numero di $[0;1]$ (in $[0;1]$ si può considerare 1 come avente l'unica rappresentazione $1 = (0, \overline{(b-1)})_b$, ma di solito si considera l'altra, ovvia, rappresentazione $1 = 1 + 0$), sia per la presenza di sviluppi impropri. In ogni caso, senza limitarsi ai numeri b-esimali di $[0; 1]$, si ha

Teorema A.2.10. *I numeri reali con più di una rappresentazione (esattamente due) sono una infinità numerabile.*

A.3 Richiami di algebra astratta

A.3.1 Alcune definizioni sulle relazioni binarie

Definizioni A.3.1.

- Una relazione binaria R è irriflessiva su A quando $\forall x \in A \neg xRx$.
- Una relazione binaria R è transitiva su A quando
$$\forall x \in A\, \forall y \in A\, \forall z \in A\, (xRy \wedge yRz) \Rightarrow xRz$$
- Una relazione binaria R è una relazione d'ordine (stretto, parziale: possono essere lasciati sottointesi) su A se è irriflessiva e transitiva. A si dice ordinato da R; se esiste una R che ordini A, esso si dice ordinabile.
- Se A è ordinato da $<_A$, un suo segmento iniziale determinato da $x \in A$ è $seg(x) = \{y \in A;\ y <_A x\}$. Se è necessario specificare, si scrive $seg(x; A; <_A)$ o simili.
- Una relazione binaria R è una relazione d'ordine (stretto) *totale* su A se vale la *legge di tricotomia*: $\forall x \in A\, \forall y \in A\, (xRy$ aut $x = y$ aut $yRx)$.
- Una relazione binaria R è una relazione d'ordine *debole* su A se si ottiene da una relazione d'ordine R_1 su A con $xRy \Longleftrightarrow (xR_1y \vee x = y)$.
- Un minimo per una relazione R d'ordine (anche debole) su A è un elemento $m \in A$ tale che $\forall x \in A(x \neq m \Rightarrow mRx)$. Un massimo per una relazione R d'ordine (anche debole) è un elemento $M \in A$ tale che $\forall x \in A(x \neq M \Rightarrow xRM)$.

- Un elemento massimale per una relazione d'ordine R (anche debole) su A è un $M' \in A$ tale che $\neg\exists x \in A(x \neq M' \wedge M'Rx)$. Analogamente per gli elementi minimali.

- Se A è debolmente ordinato da R, un suo sottoinsieme X si dice superiormente limitato da M se $\forall x \in X\ (xRM)$; se esiste un tale M, X si dice superiormente limitato; M si chiama un maggiorante di X (in A, e rispetto a R).

- Una relazione d'ordine R su A è un buon ordinamento per A se per ogni $\emptyset \neq X \subseteq A$, X ha minimo rispetto a R (principio di minimo).

Osservazioni A.3.2.
- Si noti che, per il modo in cui sono state definite, se una relazione è, poniamo, d'ordine su A, lo è anche su ogni suo sottoinsieme X.

- Minimi e massimi, se esistono, sono unici.

- Alle nozioni di sottoinsieme superiormente limitato e maggiorante corrispondono analoghe nozioni di sottoinsieme inferiormente limitato e minorante.

- Un buon ordinamento è sempre una relazione d'ordine totale. $\emptyset$ è bene ordinabile.

A.3.2 Funzioni: alcune notazioni e convenzioni

- Una corrispondenza biunivoca tra a e b è una funzione biiettiva (cioè iniettiva e suriettiva) $f : a \xrightarrow[\text{su}]{\text{1-1}} b$ e si scrive $a \overset{f}{\sim} b$. Se esiste una corrispondenza biunivoca tra a e b si dice che essi possono venire messi in corrispondenza biunivoca, o che sono equipotenti, e si scrive $a \sim b$.

- Se a e b sono ordinati da $<_a$ e $<_b$ rispettivamente, una similitudine è una corrispondenza biunivoca f tra i due insiemi tale che

$$\forall x \in a \forall y \in a(x <_a y \iff f(x) <_b f(y));$$

se una tale similitudine esiste, si dice che a e b sono simili: $a \approx b$. Se si vuole specificare f si scrive $a \overset{f}{\approx} b$. Se si vogliono specificare gli ordinamenti, si scrive $(a; <_a) \approx (b; <_b)$, eccetera. Si noti che una similitudine trasforma segmenti in segmenti:

$$a \overset{f}{\approx} b \text{ implica } \forall x \in a(f[seg(x; a; <_a)] = seg(f(x); b; <_b))$$

Bibliografia

[Abian 1972] A. Abian: *La teoria degli insiemi e l'aritmetica transfinita*, Feltrinelli, Milano 1972 (I ed. inglese 1965; trad. it.).

[Andretta 2003] A. Andretta: 'I teoremi di assolutezza in teoria degli insiemi', *Bollettino U.M.I.-La Matematica nella Società e nella Cultura*, Serie VIII **VI-A**; I parte: Aprile 2003, 57-84; II parte: Dicembre 2003, 489-507.

[Barwise-Moss 1991] J. Barwise, L. Moss: 'Hypersets', *Math. Intelligencer*, **13** n.4, 1991.

[Bottazzini 1990] U. Bottazzini: *Il flauto di Hilbert*, Utet, Torino 1990.

[Dauben 1979] J. W. Dauben: *Georg Cantor*, Harvard University Press, Cambridge (Mass.)-London 1979.

[Ebbinghaus-Flum-Thomas 1994] H.-D. Ebbinghaus, J. Flum, W. Thomas: *Mathematical Logic*, Springer-Verlag, Berlin-Heidelberg-New York 1994^2 (ed. originale 1978; trad. inglese dal tedesco).

[Edgar 1995] G. A. Edgar: *Measure, Topology and Fractal Geometry*, "Undergraduate Texts in Mathematics", Springer-Verlag, Berlin-Heidelberg-New York 1995.

[Halmos 1980] P. R. Halmos: *Teoria elementare degli insiemi*, "Collana di matematica" 7, Feltrinelli, Milano 1980 (I ed. inglese 1960; trad. it.).

[Henle 1986] J. M. Henle: *An Outline in Set Theory*, Springer, Berlin etc. 1986.

[Holmes 1998] M. R. Holmes: *Elementary set theory with a universal set*, Université catholique de Louvain-Département de Philosophie, "Cahiers du Centre de Logique" **10**, Louvain-la-Neuve 1998.

[Keisler 1976] H. J. Keisler: *Foundations of Infinitesimal Calculus*, Prindle, Weber & Schmidt 1976[1].

[Kunen 1980] K. Kunen: *Set Theory–An Introduction to Independence Proofs*, "Studies in Logic and the Foundations of Mathematics" **102**, North-Holland Publishing Co., Amsterdam-New York-Oxford 1980.

[Lolli 1991] G. Lolli: *Introduzione alla logica formale*, Il Mulino, Bologna 1991.

[Mangione 1975] C. Mangione: 'Logica e problema dei fondamenti nella seconda metà dell'Ottocento', in: L. Geymonat: *Storia del Pensiero Filosofico e Scientifico*, Vol. VI, Cap. XII, Garzanti, Milano 1975[2].

[Mendelson 1972] E. Mendelson: *Introduzione alla logica matematica*, Boringhieri, Torino 1972 (I ed. inglese 1964; trad. it.).

[Moore 1982] G. H. Moore: *Zermelo's Axiom of Choice*, "Studies in the History of Mathematics and Physical Sciences" **8**, Springer-Verlag, New York-Heidelberg-Berlin 1982

[Robert 1988] A. Robert, "Nonstandard Analysis", Wiley & Sons, New York 1988.

[Smullyan-Fitting 1996] R. M. Smullyan, M. Fitting: *Set Theory and the Continuum Problem*, "Oxford Logic Guides" **34**, Clarendon Press, Oxford 1996.

Indice analitico